Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

What CIPA requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

- CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD) at sl.universalservice.org. SLD

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

also operates a client service bureau to answer questions at 1-888-203-8100 or via email through the SLD website.

Filing a complaint

You have multiple options for filing a complaint with the FCC:

- File a complaint online at https://consumercomplaints.fcc.gov
- By phone: 1-888-CALL-FCC (1-888-225-5322); TTY: 1-888-TELL-FCC (1-888-835-5322); ASL: 1-844-432-2275
- By mail (please include your name, address, contact information and as much detail about your complaint as possible):

Federal Communications Commission
Consumer and Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
45 L Street NE
Washington, DC 20554

Alternate formats

To request this article in an alternate format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed: 12/30/19

This content is from the eCFR and is authoritative but unofficial.

Title 16 —Commercial Practices
Chapter I —Federal Trade Commission
Subchapter C —Regulations Under Specific Acts of Congress

Part 312 Children's Online Privacy Protection Rule (Coppa Rule)
- **§ 312.1** Scope of regulations in this part.
- **§ 312.2** Definitions.
- **§ 312.3** Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the internet.
- **§ 312.4** Notice.
- **§ 312.5** Parental consent.
- **§ 312.6** Right of parent to review personal information provided by a child.
- **§ 312.7** Prohibition against conditioning a child's participation on collection of personal information.
- **§ 312.8** Confidentiality, security, and integrity of personal information collected from children.
- **§ 312.9** Enforcement.
- **§ 312.10** Data retention and deletion requirements.
- **§ 312.11** Safe harbor programs.
- **§ 312.12** Voluntary Commission approval processes.
- **§ 312.13** Severability.

PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE (COPPA RULE)

Authority: 15 U.S.C. 6501 through 6506.

Source: 78 FR 4008, Jan. 17, 2013, as amended at 90 FR 16977, Apr. 22, 2025, unless otherwise noted.

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501, *et seq.*), which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the internet.

§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(1) Requesting, prompting, or encouraging a child to submit personal information online;

(2) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(3) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(1) The release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service; and

(2) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Mixed audience website or online service means a website or online service that is directed to children under the criteria set forth in paragraph (1) of the definition of *website or online service directed to children,* but that does not target children as its primary audience, and does not collect personal information from any visitor, other than for the limited purposes set forth in § 312.5(c), prior to collecting age information or using another means that is reasonably calculated, in light of available technology, to determine whether the visitor is a child. Any collection of age information, or other means of determining whether a visitor is a child, must be done in a neutral manner that does not default to a set age or encourage visitors to falsify age information.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(1) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(2) Authorizes any collection, use, and/or disclosure of the personal information.

Online contact information means an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over Internet Protocol (VOIP) identifier, a video chat user identifier, or a mobile telephone number provided the operator uses it only to send text messages to a parent in connection with obtaining parental consent.

Operator means any person who operates a website located on the internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that website or online service, where such website or online service is operated for commercial purposes involving commerce among the several States or with one or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45). Personal information is collected or maintained on behalf of an operator when:

(1) It is collected or maintained by an agent or service provider of the operator; or

(2) The operator benefits by allowing another person to collect personal information directly from users of such website or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(1) A first and last name;

(2) A home or other physical address including street name and name of a city or town;

(3) Online contact information as defined in this section;

(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(5) A telephone number;

(6) A government-issued identifier, such as a Social Security, State identification card, birth certificate, or passport number;

(7) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

(8) A photograph, video, or audio file where such file contains a child's image or voice;

(9) Geolocation information sufficient to identify street name and name of a city or town;

(10) A biometric identifier that can be used for the automated or semi-automated recognition of an individual, such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints; or

(11) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the website or online service means:

(1) Those activities necessary to:

(i) Maintain or analyze the functioning of the website or online service;

(ii) Perform network communications;

(iii) Authenticate users of, or personalize the content on, the website or online service;

(iv) Serve contextual advertising on the website or online service or cap the frequency of advertising;

(v) Protect the security or integrity of the user, website, or online service;

(vi) Ensure legal or regulatory compliance; or

(vii) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4).

(2) Provided, however, that, except as specifically permitted by paragraphs (1)(i) through (vii) of this definition, the information collected for the activities listed in paragraphs (1)(i) through (vii) of this definition cannot be used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

Third party means any person who is not:

(1) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(2) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children.

(1) In determining whether a website or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition and evidence regarding the intended audience, including marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services.

(2) A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

(3) A mixed audience website or online service shall not be deemed directed to children with regard to any visitor not identified as under 13.

(4) A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the internet.

It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must:

(a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));

(b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5);

(c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6);

(d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) ***General principles of notice.*** It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

(b) ***Direct notice to the parent.*** An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(c) ***Content of the direct notice to the parent*** —

(1) ***Content of the direct notice to the parent for purposes of obtaining consent.*** The direct notice to obtain the parent's affirmative consent to the collection, use, or disclosure of a child's personal information (including under § 312.5(c)(1)) shall set forth:

(i) If applicable, that the operator has collected the parent's or child's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

(ii) That the parent's consent is required for the collection, use, or disclosure of personal information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

(iii) The items of personal information the operator intends to collect from the child, how the operator intends to use such information, and the potential opportunities for the disclosure of personal information, should the parent provide consent;

(iv) Where the operator discloses personal information to one or more third parties, the identities or specific categories of such third parties (including the public if making it publicly available) and the purposes for such disclosure, should the parent provide consent, and that the parent can consent to the collection and use of the child's personal information without consenting to the disclosure of such personal information to third parties except to the extent such disclosure is integral to the website or online service;

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section;

(vi) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

(vii) If the operator has collected the name or online contact information of the parent or child to provide notice and obtain parental consent, that if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's or child's online contact information and the parent's or child's name from its records.

(2) ***Content of the direct notice to the parent of a child's online activities not involving the collection, use or disclosure of personal information.*** Where an operator chooses to notify a parent of a child's participation in a website or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the voluntary direct notice to the parent of a child's online activities not involving the collection, use or disclosure of personal information (required under § 312.5(c)(2)) shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information;

(ii) That the parent's online contact information will not be used or disclosed for any other purpose;

(iii) That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and

(iv) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(3) ***Content of the direct notice to the parent of operator's intent to communicate with the child multiple times.*** The direct notice to the parent of the operator's intent to communicate with the child multiple times (required under § 312.5(c)(4)) shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

(ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;

(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;

(iv) That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;

(v) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and

(vi) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(4) ***Content of the direct notice to the parent in order to protect a child's safety.*** The direct notice to the parent in order to protect a child's safety (required under § 312.5(c)(5)) shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;

(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;

(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and

(v) A hyperlink to the operator's online notice of its information practices required under paragraph (d) of this section.

(d) ***Notice on the website or online service.*** In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its website or online service, *and,* at each area of the website or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience website or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the website or online service's information practices must state the following:

(1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the website or online service. Provided that: The operators of a website or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(2) A description of what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how the operator uses such information; the operator's disclosure practices for such information, including the

identities and specific categories of any third parties to which the operator discloses personal information and the purposes for such disclosures; and the operator's data retention policy as required under § 312.10;

(3) If applicable, the specific internal operations for which the operator has collected a persistent identifier pursuant to § 312.5(c)(7); and the means the operator uses to ensure that such identifier is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose (except as specifically permitted to provide support for the internal operations of the website or online service);

(4) Where the operator collects audio files containing a child's voice pursuant to § 312.5(c)(9), a description of how the operator uses such audio files and that the operator deletes such audio files immediately after responding to the request for which they were collected; and

(5) If applicable, that the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

§ 312.5 Parental consent.

(a) ***General requirements.***

(1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties, unless such disclosure is integral to the website or online service. An operator required to give the parent this option must obtain separate verifiable parental consent to such disclosure.

(b) ***Methods for verifiable parental consent.***

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:

(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;

(ii) Requiring a parent, in connection with a transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(iii) Having a parent call a toll-free telephone number staffed by trained personnel;

(iv) Having a parent connect to trained personnel via video-conference;

(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete;

(vi) Verifying a parent's identity using knowledge-based authentication provided:

(A) the verification process uses dynamic, multiple-choice questions, where there are a reasonable number of questions with an adequate number of possible answers such that the probability of correctly guessing the answers is low; and

(B) the questions are of sufficient difficulty that a child age 12 or younger in the parent's household could not reasonably ascertain the answers;

(vii) Having a parent submit a government-issued photographic identification that is verified to be authentic and is compared against an image of the parent's face taken with a phone camera or webcam using facial recognition technology and confirmed by personnel trained to confirm that the photos match; provided that the parent's identification and images are promptly deleted by the operator from its records after the match is confirmed; or

(viii) Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

(ix) Provided that, an operator that does not "disclose" (as defined by § 312.2) children's personal information, may use a text message coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory text message to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier text message.

(3) ***Safe harbor approval of parental consent methods.*** A safe harbor program approved by the Commission under § 312.11 may approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) of this section where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1) of this section.

(c) ***Exceptions to prior parental consent.*** Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child except as set forth in this paragraph:

(1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2);

(3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

(4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered;

(5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4);

(6) Where the purpose of collecting a child's name and online contact information is to:

(i) Protect the security or integrity of the website or online service;

(ii) Take precautions against liability;

(iii) Respond to judicial process; or

(iv) To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not used for any other purpose;

(7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. In such case, the operator shall provide notice under § 312.4(d)(3);

(8) Where an operator covered under paragraph (2) of the definition of *website or online service directed to children* in § 312.2 collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4; or

(9) Where an operator collects an audio file containing a child's voice, and no other personal information, for use in responding to a child's specific request and where the operator does not use such information for any other purpose, does not disclose it, and deletes it immediately after responding to the child's request. In such case, there also shall be no obligation to provide a direct notice, but notice shall be required under § 312.4(d).

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

(a) The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

(b) At a minimum, the operator must establish, implement, and maintain a written information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities. To satisfy this requirement, the operator must:

(1) Designate one or more employees to coordinate the operator's information security program;

(2) Identify and, at least annually, perform additional assessments to identify internal and external risks to the confidentiality, security, and integrity of personal information collected from children and the sufficiency of any safeguards in place to control such risks;

(3) Design, implement, and maintain safeguards to control risks identified through the risk assessments required under paragraph (b)(2) of this section. Each safeguard must be based on the volume and sensitivity of the children's personal information that is at risk, and the likelihood that the risk could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information;

(4) Regularly test and monitor the effectiveness of the safeguards in place to control risks identified through the risk assessments required under paragraph (b)(2) of this section; and

(5) At least annually, evaluate and modify the information security program to address identified risks, results of required testing and monitoring, new or more efficient technological or operational methods to control for identified risks, or any other circumstances that an operator knows or has reason to know may have a material impact on its information security program or any safeguards in place to protect personal information collected from children.

(c) Before allowing other operators, service providers, or third parties to collect or maintain personal information from children on the operator's behalf, or before releasing children's personal information to such entities, the operator must take reasonable steps to determine that such entities are capable of maintaining the confidentiality, security, and integrity of the information and must obtain written assurances that such entities will employ reasonable measures to maintain the confidentiality, security, and integrity of the information.

§ 312.9 Enforcement.

Subject to sections 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502(a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Data retention and deletion requirements.

An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the specific purpose(s) for which the information was collected. When such information is no longer reasonably necessary for the purposes for which it was collected, the operator must delete the information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion. Personal information collected online from a child may not be retained indefinitely. At a minimum, the operator must establish, implement, and maintain a written data retention policy that sets forth the purposes for which children's personal information is collected, the business need for retaining such information, and a timeframe for deletion of such information. The operator must provide its written data retention policy addressing personal information collected from children in the notice on the website or online service provided in accordance with § 312.4(d).

§ 312.11 Safe harbor programs.

(a) ***In general.*** Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) ***Criteria for approval of self-regulatory program guidelines.*** Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually,

of each subject operator's information privacy and security policies, practices, and representations. The assessment mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self-regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) ***Request for Commission approval of self-regulatory program guidelines.*** A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) How the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) How the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) of this section provide effective enforcement of the requirements of this part.

(d) ***Reporting and recordkeeping requirements.*** Approved safe harbor programs shall:

(1) By October 22, 2025, and annually thereafter, submit a report to the Commission that identifies each subject operator and all approved websites or online services, as well as any subject operators that have left the safe harbor program. The report must also contain, at a minimum:

(i) a narrative description of the safe harbor program's business model, including whether it provides additional services such as training to subject operators;

(ii) copies of each consumer complaint related to each subject operator's violation of a safe harbor program's guidelines;

(iii) an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section;

(iv) a description of each disciplinary action taken against any subject operator under paragraph (b)(3) of this section, as well as a description of the process for determining whether a subject operator is subject to discipline; and

(v) a description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(3);

(2) Promptly respond to Commission requests for additional information;

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section; and

(4) No later than July 21, 2025, publicly post on each of the approved safe harbor program's websites and online services a list of all current subject operators and, for each such operator, list each certified website or online service. Approved safe harbor programs shall update this list every six months thereafter to reflect any changes to the approved safe harbor programs' subject operators or their applicable websites and online services.

(e) ***Post-approval modifications to self-regulatory program guidelines.*** Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2) of this section. The statement required under paragraph (c)(4) of this section must describe how the proposed changes affect existing provisions of the guidelines.

(f) ***Review of self-regulatory program guidelines.*** No later than April 22, 2028, and every three years thereafter, approved safe harbor programs shall submit to the Commission a report detailing the safe harbor program's technological capabilities and mechanisms for assessing subject operators' fitness for membership in the safe harbor program.

(g) ***Revocation of approval of self-regulatory program guidelines.*** The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs shall, by October 22, 2025, submit proposed modifications to their guidelines.

(h) ***Operators' participation in a safe harbor program.*** An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non-compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3) of this section. [78 FR 4008, Jan. 17, 2013, as amended at 78 FR 76986, Dec. 20, 2013]

§ 312.12 Voluntary Commission approval processes.

(a) ***Parental consent methods.*** An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in § 312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

(b) ***Support for the internal operations of the website or online service.*** An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for the internal operations of the website or online service. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for the internal operations of the website or online service, and an analysis of their potential effects on children's online privacy. The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

This content is from the eCFR and is authoritative but unofficial.

Title 34 —Education
Subtitle A —Office of the Secretary, Department of Education

Part 99 Family Educational Rights and Privacy

Subpart A General

§ 99.1 To which educational agencies or institutions do these regulations apply?
§ 99.2 What is the purpose of these regulations?
§ 99.3 What definitions apply to these regulations?
§ 99.4 What are the rights of parents?
§ 99.5 What are the rights of students?
§ 99.6 [Reserved]
§ 99.7 What must an educational agency or institution include in its annual notification?
§ 99.8 What provisions apply to records of a law enforcement unit?

Subpart B What Are the Rights of Inspection and Review of Education Records?

§ 99.10 What rights exist for a parent or eligible student to inspect and review education records?
§ 99.11 May an educational agency or institution charge a fee for copies of education records?
§ 99.12 What limitations exist on the right to inspect and review records?

Subpart C What Are the Procedures for Amending Education Records?

§ 99.20 How can a parent or eligible student request amendment of the student's education records?
§ 99.21 Under what conditions does a parent or eligible student have the right to a hearing?
§ 99.22 What minimum requirements exist for the conduct of a hearing?

Subpart D May an Educational Agency or Institution Disclose Personally Identifiable Information From Education Records?

§ 99.30 Under what conditions is prior consent required to disclose information?
§ 99.31 Under what conditions is prior consent not required to disclose information?
§ 99.32 What recordkeeping requirements exist concerning requests and disclosures?
§ 99.33 What limitations apply to the redisclosure of information?
§ 99.34 What conditions apply to disclosure of information to other educational agencies or institutions?
§ 99.35 What conditions apply to disclosure of information for Federal or State program purposes?
§ 99.36 What conditions apply to disclosure of information in health and safety emergencies?
§ 99.37 What conditions apply to disclosing directory information?
§ 99.38 What conditions apply to disclosure of information as permitted by State statute adopted after November 19, 1974, concerning the juvenile justice system?

§ 99.39 What definitions apply to the nonconsensual disclosure of records by postsecondary educational institutions in connection with disciplinary proceedings concerning crimes of violence or non-forcible sex offenses?

Subpart E What Are the Enforcement Procedures?

§ 99.60 What functions has the Secretary delegated to the Office and to the Office of Administrative Law Judges?

§ 99.61 What responsibility does an educational agency or institution, a recipient of Department funds, or a third party outside of an educational agency or institution have concerning conflict with State or local laws?

§ 99.62 What information must an educational agency or institution or other recipient of Department funds submit to the Office?

§ 99.63 Where are complaints filed?

§ 99.64 What is the investigation procedure?

§ 99.65 What is the content of the notice of investigation issued by the Office?

§ 99.66 What are the responsibilities of the Office in the enforcement process?

§ 99.67 How does the Secretary enforce decisions?

Appendix A to Part 99

Crimes of Violence Definitions

PART 99—FAMILY EDUCATIONAL RIGHTS AND PRIVACY

Authority: 20 U.S.C. 1232g, unless otherwise noted.

Source: 53 FR 11943, Apr. 11, 1988, unless otherwise noted.

Subpart A—General

§ 99.1 To which educational agencies or institutions do these regulations apply?

(a) Except as otherwise noted in § 99.10, this part applies to an educational agency or institution to which funds have been made available under any program administered by the Secretary, if—

(1) The educational institution provides educational services or instruction, or both, to students; or

(2) The educational agency is authorized to direct and control public elementary or secondary, or postsecondary educational institutions.

(b) This part does not apply to an educational agency or institution solely because students attending that agency or institution receive non-monetary benefits under a program referenced in paragraph (a) of this section, if no funds under that program are made available to the agency or institution.

(c) The Secretary considers funds to be made available to an educational agency or institution of funds under one or more of the programs referenced in paragraph (a) of this section—

(1) Are provided to the agency or institution by grant, cooperative agreement, contract, subgrant, or subcontract; or

(2) Are provided to students attending the agency or institution and the funds may be paid to the agency or institution by those students for educational purposes, such as under the Pell Grant Program and the Guaranteed Student Loan Program (titles IV-A-1 and IV-B, respectively, of the Higher Education Act of 1965, as amended).

(d) If an educational agency or institution receives funds under one or more of the programs covered by this section, the regulations in this part apply to the recipient as a whole, including each of its components (such as a department within a university).

(Authority: 20 U.S.C. 1232g)

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59295, Nov. 21, 1996; 65 FR 41852, July 6, 2000]

§ 99.2 What is the purpose of these regulations?

The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.

(Authority: 20 U.S.C. 1232g)

Note to § 99.2: 34 CFR 300.610 through 300.626 contain requirements regarding the confidentiality of information relating to children with disabilities who receive evaluations, services or other benefits under Part B of the Individuals with Disabilities Education Act (IDEA). 34 CFR 303.402 and 303.460 identify the confidentiality of information requirements regarding children and infants and toddlers with disabilities and their families who receive evaluations, services, or other benefits under Part C of IDEA. 34 CFR 300.610 through 300.627 contain the confidentiality of information requirements that apply to personally identifiable data, information, and records collected or maintained pursuant to Part B of the IDEA.

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59295, Nov. 21, 1996; 73 FR 74851, Dec. 9, 2008]

§ 99.3 What definitions apply to these regulations?

The following definitions apply to this part:

Act means the Family Educational Rights and Privacy Act of 1974, as amended, enacted as section 444 of the General Education Provisions Act.

(Authority: 20 U.S.C. 1232g)

Attendance includes, but is not limited to—

(a) Attendance in person or by paper correspondence, videoconference, satellite, Internet, or other electronic information and telecommunications technologies for students who are not physically present in the classroom; and

(b) The period during which a person is working under a work-study program.

(Authority: 20 U.S.C. 1232g)

Authorized representative means any entity or individual designated by a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) to conduct—with respect to Federal- or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs.

(Authority: 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5))

Biometric record, as used in the definition of *personally identifiable information,* means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

(Authority: 20 U.S.C. 1232g)

Dates of attendance.

(a) The term means the period of time during which a student attends or attended an educational agency or institution. Examples of dates of attendance include an academic year, a spring semester, or a first quarter.

(b) The term does not include specific daily records of a student's attendance at an educational agency or institution.

(Authority: 20 U.S.C. 1232g(a)(5)(A))

Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

(a) Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (*e.g.,* undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

(b) Directory information does not include a student's—

(1) Social security number; or

(2) Student identification (ID) number, except as provided in paragraph (c) of this definition.

(c) In accordance with paragraphs (a) and (b) of this definition, directory information includes—

(1) A student ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user; and

(2) A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

(Authority: 20 U.S.C. 1232g(a)(5)(A))

Disciplinary action or proceeding means the investigation, adjudication, or imposition of sanctions by an educational agency or institution with respect to an infraction or violation of the internal rules of conduct applicable to students of the agency or institution.

Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.

(Authority: 20 U.S.C. 1232g(b)(1) and (b)(2))

Early childhood education program means—

(a) A Head Start program or an Early Head Start program carried out under the Head Start Act (42 U.S.C. 9831 *et seq.*), including a migrant or seasonal Head Start program, an Indian Head Start program, or a Head Start program or an Early Head Start program that also receives State funding;

(b) A State licensed or regulated child care program; or

(c) A program that—

(1) Serves children from birth through age six that addresses the children's cognitive (including language, early literacy, and early mathematics), social, emotional, and physical development; and

(2) Is—

(i) A State prekindergarten program;

(ii) A program authorized under section 619 or part C of the Individuals with Disabilities Education Act; or

(iii) A program operated by a local educational agency.

Educational agency or institution means any public or private agency or institution to which this part applies under § 99.1(a).

(Authority: 20 U.S.C. 1232g(a)(3))

Education program means any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.

(Authority: 20 U.S.C. 1232g(b)(3), (b)(5))

Education records.

(a) The term means those records that are:

(1) Directly related to a student; and

(2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

(b) The term does not include:

(1) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.

(2) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of § 99.8.

(3)

(i) Records relating to an individual who is employed by an educational agency or institution, that:

(A) Are made and maintained in the normal course of business;

(B) Relate exclusively to the individual in that individual's capacity as an employee; and

(C) Are not available for use for any other purpose.

(ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition.

(4) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:

(i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;

(ii) Made, maintained, or used only in connection with treatment of the student; and

(iii) Disclosed only to individuals providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution; and

(5) Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.

(6) Grades on peer-graded papers before they are collected and recorded by a teacher.

(Authority: 20 U.S.C. 1232g(a)(4))

Eligible student means a student who has reached 18 years of age or is attending an institution of postsecondary education.

(Authority: 20 U.S.C. 1232g(d))

Institution of postsecondary education means an institution that provides education to students beyond the secondary school level; "secondary school level" means the educational level (not beyond grade 12) at which secondary education is provided as determined under State law.

(Authority: 20 U.S.C. 1232g(d))

Parent means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.

(Authority: 20 U.S.C. 1232g)

Party means an individual, agency, institution, or organization.

(Authority: 20 U.S.C. 1232g(b)(4)(A))

Personally Identifiable Information

The term includes, but is not limited to—

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's social security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

(Authority: 20 U.S.C. 1232g)

Record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

(Authority: 20 U.S.C. 1232g)

Secretary means the Secretary of the U.S. Department of Education or an official or employee of the Department of Education acting for the Secretary under a delegation of authority.

(Authority: 20 U.S.C. 1232g)

Student, except as otherwise specifically provided in this part, means any individual who is or has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records.

(Authority: 20 U.S.C. 1232g(a)(6))

[53 FR 11943, Apr. 11, 1988, as amended at 60 FR 3468, Jan. 17, 1995; 61 FR 59295, Nov. 21, 1996; 65 FR 41852, July 6, 2000; 73 FR 74851, Dec. 9, 2008; 76 FR 75641, Dec. 2, 2011]

§ 99.4 What are the rights of parents?

An educational agency or institution shall give full rights under the Act to either parent, unless the agency or institution has been provided with evidence that there is a court order, State statute, or legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights.

(Authority: 20 U.S.C. 1232g)

§ 99.5 What are the rights of students?

(a)

(1) When a student becomes an eligible student, the rights accorded to, and consent required of, parents under this part transfer from the parents to the student.

(2) Nothing in this section prevents an educational agency or institution from disclosing education records, or personally identifiable information from education records, to a parent without the prior written consent of an eligible student if the disclosure meets the conditions in § 99.31(a)(8), § 99.31(a)(10), § 99.31(a)(15), or any other provision in § 99.31(a).

(b) The Act and this part do not prevent educational agencies or institutions from giving students rights in addition to those given to parents.

(c) An individual who is or has been a student at an educational institution and who applies for admission at another component of that institution does not have rights under this part with respect to records maintained by that other component, including records maintained in connection with the student's application for admission, unless the student is accepted and attends that other component of the institution.

(Authority: 20 U.S.C. 1232g(d))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3188, Jan. 7, 1993; 65 FR 41853, July 6, 2000; 73 FR 74852, Dec. 9, 2008]

§ 99.6 [Reserved]

§ 99.7 What must an educational agency or institution include in its annual notification?

(a)

(1) Each educational agency or institution shall annually notify parents of students currently in attendance, or eligible students currently in attendance, of their rights under the Act and this part.

(2) The notice must inform parents or eligible students that they have the right to—

(i) Inspect and review the student's education records;

(ii) Seek amendment of the student's education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights;

(iii) Consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that the Act and § 99.31 authorize disclosure without consent; and

(iv) File with the Department a complaint under §§ 99.63 and 99.64 concerning alleged failures by the educational agency or institution to comply with the requirements of the Act and this part.

(3) The notice must include all of the following:

(i) The procedure for exercising the right to inspect and review education records.

(ii) The procedure for requesting amendment of records under § 99.20.

(iii) If the educational agency or institution has a policy of disclosing education records under § 99.31(a)(1), a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

(b) An educational agency or institution may provide this notice by any means that are reasonably likely to inform the parents or eligible students of their rights.

(1) An educational agency or institution shall effectively notify parents or eligible students who are disabled.

(2) An agency or institution of elementary or secondary education shall effectively notify parents who have a primary or home language other than English.

(Approved by the Office of Management and Budget under control number 1880-0508)

(Authority: 20 U.S.C. 1232g (e) and (f))

[61 FR 59295, Nov. 21, 1996]

§ 99.8 What provisions apply to records of a law enforcement unit?

(a)

(1) ***Law enforcement unit*** means any individual, office, department, division, or other component of an educational agency or institution, such as a unit of commissioned police officers or non-commissioned security guards, that is officially authorized or designated by that agency or institution to—

(i) Enforce any local, State, or Federal law, or refer to appropriate authorities a matter for enforcement of any local, State, or Federal law against any individual or organization other than the agency or institution itself; or

(ii) Maintain the physical security and safety of the agency or institution.

(2) A component of an educational agency or institution does not lose its status as a *law enforcement unit* if it also performs other, non-law enforcement functions for the agency or institution, including investigation of incidents or conduct that constitutes or leads to a disciplinary action or proceedings against the student.

(b)

(1) Records of a law enforcement unit means those records, files, documents, and other materials that are—

(i) Created by a law enforcement unit;

(ii) Created for a law enforcement purpose; and

(iii) Maintained by the law enforcement unit.

(2) Records of a law enforcement unit does not mean—

(i) Records created by a law enforcement unit for a law enforcement purpose that are maintained by a component of the educational agency or institution other than the law enforcement unit; or

(ii) Records created and maintained by a law enforcement unit exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the educational agency or institution.

(c)

(1) Nothing in the Act prohibits an educational agency or institution from contacting its law enforcement unit, orally or in writing, for the purpose of asking that unit to investigate a possible violation of, or to enforce, any local, State, or Federal law.

(2) Education records, and personally identifiable information contained in education records, do not lose their status as education records and remain subject to the Act, including the disclosure provisions of § 99.30, while in the possession of the law enforcement unit.

(d) The Act neither requires nor prohibits the disclosure by an educational agency or institution of its law enforcement unit records.

(Authority: 20 U.S.C. 1232g(a)(4)(B)(ii))

[60 FR 3469, Jan. 17, 1995]

Subpart B—What Are the Rights of Inspection and Review of Education Records?

§ 99.10 What rights exist for a parent or eligible student to inspect and review education records?

(a) Except as limited under § 99.12, a parent or eligible student must be given the opportunity to inspect and review the student's education records. This provision applies to—

(1) Any educational agency or institution; and

(2) Any State educational agency (SEA) and its components.

(i) For the purposes of subpart B of this part, an SEA and its components constitute an educational agency or institution.

(ii) An SEA and its components are subject to subpart B of this part if the SEA maintains education records on students who are or have been in attendance at any school of an educational agency or institution subject to the Act and this part.

(b) The educational agency or institution, or SEA or its component, shall comply with a request for access to records within a reasonable period of time, but not more than 45 days after it has received the request.

(c) The educational agency or institution, or SEA or its component shall respond to reasonable requests for explanations and interpretations of the records.

(d) If circumstances effectively prevent the parent or eligible student from exercising the right to inspect and review the student's education records, the educational agency or institution, or SEA or its component, shall—

(1) Provide the parent or eligible student with a copy of the records requested; or

(2) Make other arrangements for the parent or eligible student to inspect and review the requested records.

(e) The educational agency or institution, or SEA or its component shall not destroy any education records if there is an outstanding request to inspect and review the records under this section.

(f) While an education agency or institution is not required to give an eligible student access to treatment records under paragraph (b)(4) of the definition of *Education records* in § 99.3, the student may have those records reviewed by a physician or other appropriate professional of the student's choice.

(Authority: 20 U.S.C. 1232g(a)(1) (A) and (B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

§ 99.11 May an educational agency or institution charge a fee for copies of education records?

(a) Unless the imposition of a fee effectively prevents a parent or eligible student from exercising the right to inspect and review the student's education records, an educational agency or institution may charge a fee for a copy of an education record which is made for the parent or eligible student.

(b) An educational agency or institution may not charge a fee to search for or to retrieve the education records of a student.

(Authority: 20 U.S.C. 1232g(a)(1))

§ 99.12 What limitations exist on the right to inspect and review records?

(a) If the education records of a student contain information on more than one student, the parent or eligible student may inspect and review or be informed of only the specific information about that student.

(b) A postsecondary institution does not have to permit a student to inspect and review education records that are:

(1) Financial records, including any information those records contain, of his or her parents;

(2) Confidential letters and confidential statements of recommendation placed in the education records of the student before January 1, 1975, as long as the statements are used only for the purposes for which they were specifically intended; and

(3) Confidential letters and confidential statements of recommendation placed in the student's education records after January 1, 1975, if:

(i) The student has waived his or her right to inspect and review those letters and statements; and

(ii) Those letters and statements are related to the student's:

(A) Admission to an educational institution;

(B) Application for employment; or

(C) Receipt of an honor or honorary recognition.

(c)

(1) A waiver under paragraph (b)(3)(i) of this section is valid only if:

(i) The educational agency or institution does not require the waiver as a condition for admission to or receipt of a service or benefit from the agency or institution; and

(ii) The waiver is made in writing and signed by the student, regardless of age.

(2) If a student has waived his or her rights under paragraph (b)(3)(i) of this section, the educational institution shall:

(i) Give the student, on request, the names of the individuals who provided the letters and statements of recommendation; and

(ii) Use the letters and statements of recommendation only for the purpose for which they were intended.

(3)

(i) A waiver under paragraph (b)(3)(i) of this section may be revoked with respect to any actions occurring after the revocation.

(ii) A revocation under paragraph (c)(3)(i) of this section must be in writing.

(Authority: 20 U.S.C. 1232g(a)(1) (A), (B), (C), and (D))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

Subpart C—What Are the Procedures for Amending Education Records?

§ 99.20 How can a parent or eligible student request amendment of the student's education records?

(a) If a parent or eligible student believes the education records relating to the student contain information that is inaccurate, misleading, or in violation of the student's rights of privacy, he or she may ask the educational agency or institution to amend the record.

(b) The educational agency or institution shall decide whether to amend the record as requested within a reasonable time after the agency or institution receives the request.

(c) If the educational agency or institution decides not to amend the record as requested, it shall inform the parent or eligible student of its decision and of his or her right to a hearing under § 99.21.

(Authority: 20 U.S.C. 1232g(a)(2))

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

§ 99.21 Under what conditions does a parent or eligible student have the right to a hearing?

(a) An educational agency or institution shall give a parent or eligible student, on request, an opportunity for a hearing to challenge the content of the student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation of the privacy rights of the student.

(b)

(1) If, as a result of the hearing, the educational agency or institution decides that the information is inaccurate, misleading, or otherwise in violation of the privacy rights of the student, it shall:

(i) Amend the record accordingly; and

(ii) Inform the parent or eligible student of the amendment in writing.

(2) If, as a result of the hearing, the educational agency or institution decides that the information in the education record is not inaccurate, misleading, or otherwise in violation of the privacy rights of the student, it shall inform the parent or eligible student of the right to place a statement in the record commenting on the contested information in the record or stating why he or she disagrees with the decision of the agency or institution, or both.

(c) If an educational agency or institution places a statement in the education records of a student under paragraph (b)(2) of this section, the agency or institution shall:

(1) Maintain the statement with the contested part of the record for as long as the record is maintained; and

(2) Disclose the statement whenever it discloses the portion of the record to which the statement relates.

(Authority: 20 U.S.C. 1232g(a)(2))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

§ 99.22 What minimum requirements exist for the conduct of a hearing?

The hearing required by § 99.21 must meet, at a minimum, the following requirements:

(a) The educational agency or institution shall hold the hearing within a reasonable time after it has received the request for the hearing from the parent or eligible student.

(b) The educational agency or institution shall give the parent or eligible student notice of the date, time, and place, reasonably in advance of the hearing.

(c) The hearing may be conducted by any individual, including an official of the educational agency or institution, who does not have a direct interest in the outcome of the hearing.

(d) The educational agency or institution shall give the parent or eligible student a full and fair opportunity to present evidence relevant to the issues raised under § 99.21. The parent or eligible student may, at their own expense, be assisted or represented by one or more individuals of his or her own choice, including an attorney.

(e) The educational agency or institution shall make its decision in writing within a reasonable period of time after the hearing.

(f) The decision must be based solely on the evidence presented at the hearing, and must include a summary of the evidence and the reasons for the decision.

(Authority: 20 U.S.C. 1232g(a)(2))

Subpart D—May an Educational Agency or Institution Disclose Personally Identifiable Information From Education Records?

§ 99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31.

(b) The written consent must:

(1) Specify the records that may be disclosed;

(2) State the purpose of the disclosure; and

(3) Identify the party or class of parties to whom the disclosure may be made.

(c) When a disclosure is made under paragraph (a) of this section:

(1) If a parent or eligible student so requests, the educational agency or institution shall provide him or her with a copy of the records disclosed; and

(2) If the parent of a student who is not an eligible student so requests, the agency or institution shall provide the student with a copy of the records disclosed.

(d) "Signed and dated written consent" under this part may include a record and signature in electronic form that—

(1) Identifies and authenticates a particular person as the source of the electronic consent; and

(2) Indicates such person's approval of the information contained in the electronic consent.

(Authority: 20 U.S.C. 1232g (b)(1) and (b)(2)(A))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 69 FR 21671, Apr. 21, 2004]

§ 99.31 Under what conditions is prior consent not required to disclose information?

(a) An educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by § 99.30 if the disclosure meets one or more of the following conditions:

(1)

(i)

(A) The disclosure is to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests.

(B) A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party—

(*1*) Performs an institutional service or function for which the agency or institution would otherwise use employees;

(*2*) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and

(*3*) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

(ii) An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section.

(2) The disclosure is, subject to the requirements of § 99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

Note: Section 4155(b) of the No Child Left Behind Act of 2001, 20 U.S.C. 7165(b), requires each State to assure the Secretary of Education that it has a procedure in place to facilitate the transfer of disciplinary records with respect to a suspension or expulsion of a student by a local educational agency to any private or public elementary or secondary school in which the student is subsequently enrolled or seeks, intends, or is instructed to enroll.

(3) The disclosure is, subject to the requirements of § 99.35, to authorized representatives of—

(i) The Comptroller General of the United States;

(ii) The Attorney General of the United States;

(iii) The Secretary; or

(iv) State and local educational authorities.

(4)

(i) The disclosure is in connection with financial aid for which the student has applied or which the student has received, if the information is necessary for such purposes as to:

(A) Determine eligibility for the aid;

(B) Determine the amount of the aid;

(C) Determine the conditions for the aid; or

(D) Enforce the terms and conditions of the aid.

(ii) As used in paragraph (a)(4)(i) of this section, *financial aid* means a payment of funds provided to an individual (or a payment in kind of tangible or intangible property to the individual) that is conditioned on the individual's attendance at an educational agency or institution.

(Authority: 20 U.S.C. 1232g(b)(1)(D))

(5)

(i) The disclosure is to State and local officials or authorities to whom this information is specifically—

(A) Allowed to be reported or disclosed pursuant to State statute adopted before November 19, 1974, if the allowed reporting or disclosure concerns the juvenile justice system and the system's ability to effectively serve the student whose records are released; or

(B) Allowed to be reported or disclosed pursuant to State statute adopted after November 19, 1974, subject to the requirements of § 99.38.

(ii) Paragraph (a)(5)(i) of this section does not prevent a State from further limiting the number or type of State or local officials to whom disclosures may be made under that paragraph.

(6)

(i) The disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions to:

(A) Develop, validate, or administer predictive tests;

(B) Administer student aid programs; or

(C) Improve instruction.

(ii) Nothing in the Act or this part prevents a State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section from entering into agreements with organizations conducting studies under paragraph (a)(6)(i) of this section and redisclosing personally identifiable information from education records on behalf of educational agencies and institutions that disclosed the information to the State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section in accordance with the requirements of § 99.33(b).

(iii) An educational agency or institution may disclose personally identifiable information under paragraph (a)(6)(i) of this section, and a State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section may redisclose personally identifiable information under paragraph (a)(6)(i) and (a)(6)(ii) of this section, only if—

(A) The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;

(B) The information is destroyed when no longer needed for the purposes for which the study was conducted; and

(C) The educational agency or institution or the State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section enters into a written agreement with the organization that—

(*1*) Specifies the purpose, scope, and duration of the study or studies and the information to be disclosed;

(*2*) Requires the organization to use personally identifiable information from education records only to meet the purpose or purposes of the study as stated in the written agreement;

(*3*) Requires the organization to conduct the study in a manner that does not permit personal identification of parents and students, as defined in this part, by anyone other than representatives of the organization with legitimate interests;

and

(*4*) Requires the organization to destroy all personally identifiable information when the information is no longer needed for the purposes for which the study was conducted and specifies the time period in which the information must be destroyed.

(iv) An educational agency or institution or State or local educational authority or Federal agency headed by an official listed in paragraph (a)(3) of this section is not required to initiate a study or agree with or endorse the conclusions or results of the study.

(v) For the purposes of paragraph (a)(6) of this section, the term *organization* includes, but is not limited to, Federal, State, and local agencies, and independent organizations.

(7) The disclosure is to accrediting organizations to carry out their accrediting functions.

(8) The disclosure is to parents, as defined in § 99.3, of a dependent student, as defined in section 152 of the Internal Revenue Code of 1986.

(9)

(i) The disclosure is to comply with a judicial order or lawfully issued subpoena.

(ii) The educational agency or institution may disclose information under paragraph (a)(9)(i) of this section only if the agency or institution makes a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action, unless the disclosure is in compliance with—

(A) A Federal grand jury subpoena and the court has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed;

(B) Any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed; or

(C) An *ex parte* court order obtained by the United States Attorney General (or designee not lower than an Assistant Attorney General) concerning investigations or prosecutions of an offense listed in 18 U.S.C. 2332b(g)(5)(B) or an act of domestic or international terrorism as defined in 18 U.S.C. 2331.

(iii)

(A) If an educational agency or institution initiates legal action against a parent or student, the educational agency or institution may disclose to the court, without a court order or subpoena, the education records of the student that are relevant for the educational agency or institution to proceed with the legal action as plaintiff.

(B) If a parent or eligible student initiates legal action against an educational agency or institution, the educational agency or institution may disclose to the court, without a court order or subpoena, the student's education records that are relevant for the educational agency or institution to defend itself.

(10) The disclosure is in connection with a health or safety emergency, under the conditions described in § 99.36.

(11) The disclosure is information the educational agency or institution has designated as "directory information", under the conditions described in § 99.37.

(12) The disclosure is to the parent of a student who is not an eligible student or to the student.

(13) The disclosure, subject to the requirements in § 99.39, is to a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense. The disclosure may only include the final results of the disciplinary proceeding conducted by the institution of postsecondary education with respect to that alleged crime or offense. The institution may disclose the final results of the disciplinary proceeding, regardless of whether the institution concluded a violation was committed.

(14)

(i) The disclosure, subject to the requirements in § 99.39, is in connection with a disciplinary proceeding at an institution of postsecondary education. The institution must not disclose the final results of the disciplinary proceeding unless it determines that—

(A) The student is an alleged perpetrator of a crime of violence or non-forcible sex offense; and

(B) With respect to the allegation made against him or her, the student has committed a violation of the institution's rules or policies.

(ii) The institution may not disclose the name of any other student, including a victim or witness, without the prior written consent of the other student.

(iii) This section applies only to disciplinary proceedings in which the final results were reached on or after October 7, 1998.

(15)

(i) The disclosure is to a parent of a student at an institution of postsecondary education regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the institution, governing the use or possession of alcohol or a controlled substance if—

(A) The institution determines that the student has committed a disciplinary violation with respect to that use or possession; and

(B) The student is under the age of 21 at the time of the disclosure to the parent.

(ii) Paragraph (a)(15) of this section does not supersede any provision of State law that prohibits an institution of postsecondary education from disclosing information.

(16) The disclosure concerns sex offenders and other individuals required to register under section 170101 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. 14071, and the information was provided to the educational agency or institution under 42 U.S.C. 14071 and applicable Federal guidelines.

(b)

(1) ***De-identified records and information.*** An educational agency or institution, or a party that has received education records or information from education records under this part, may release the records or information without the consent required by § 99.30 after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information.

(2) An educational agency or institution, or a party that has received education records or information from education records under this part, may release de-identified student level data from education records for the purpose of education research by attaching a code to each record that may allow the recipient to match information received from the same source, provided that—

(i) An educational agency or institution or other party that releases de-identified data under paragraph (b)(2) of this section does not disclose any information about how it generates and assigns a record code, or that would allow a recipient to identify a student based on a record code;

(ii) The record code is used for no purpose other than identifying a de-identified record for purposes of education research and cannot be used to ascertain personally identifiable information about a student; and

(iii) The record code is not based on a student's social security number or other personal information.

(c) An educational agency or institution must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses personally identifiable information from education records.

(d) Paragraphs (a) and (b) of this section do not require an educational agency or institution or any other party to disclose education records or information from education records to any party except for parties under paragraph (a)(12) of this section.

(Authority: 20 U.S.C. 1232g(a)(5)(A), (b), (h), (i), and (j)).

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 61 FR 59296, Nov. 21, 1996; 65 FR 41853, July 6, 2000; 73 FR 74852, Dec. 9, 2008; 74 FR 401, Jan. 6, 2009; 76 FR 75641, Dec. 2, 2011]

§ 99.32 What recordkeeping requirements exist concerning requests and disclosures?

(a)

(1) An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in § 99.31(a)(3) that may make further disclosures of personally identifiable information from the student's education records without consent under § 99.33(b).

(2) The agency or institution shall maintain the record with the education records of the student as long as the records are maintained.

(3) For each request or disclosure the record must include:

(i) The parties who have requested or received personally identifiable information from the education records; and

(ii) The legitimate interests the parties had in requesting or obtaining the information.

(4) An educational agency or institution must obtain a copy of the record of further disclosures maintained under paragraph (b)(2) of this section and make it available in response to a parent's or eligible student's request to review the record required under paragraph (a)(1) of this section.

(5) An educational agency or institution must record the following information when it discloses personally identifiable information from education records under the health or safety emergency exception in § 99.31(a)(10) and § 99.36:

(i) The articulable and significant threat to the health or safety of a student or other individuals that formed the basis for the disclosure; and

(ii) The parties to whom the agency or institution disclosed the information.

(b)

(1) Except as provided in paragraph (b)(2) of this section, if an educational agency or institution discloses personally identifiable information from education records with the understanding authorized under § 99.33(b), the record of the disclosure required under this section must include:

(i) The names of the additional parties to which the receiving party may disclose the information on behalf of the educational agency or institution; and

(ii) The legitimate interests under § 99.31 which each of the additional parties has in requesting or obtaining the information.

(2)

(i) A State or local educational authority or Federal official or agency listed in § 99.31(a)(3) that makes further disclosures of information from education records under § 99.33(b) must record the names of the additional parties to which it discloses information on behalf of an educational agency or institution and their legitimate interests in the information under § 99.31 if the information was received from:

(A) An educational agency or institution that has not recorded the further disclosures under paragraph (b)(1) of this section; or

(B) Another State or local educational authority or Federal official or agency listed in § 99.31(a)(3).

(ii) A State or local educational authority or Federal official or agency that records further disclosures of information under paragraph (b)(2)(i) of this section may maintain the record by the student's class, school, district, or other appropriate grouping rather than by the name of the student.

(iii) Upon request of an educational agency or institution, a State or local educational authority or Federal official or agency listed in § 99.31(a)(3) that maintains a record of further disclosures under paragraph (b)(2)(i) of this section must provide a copy of the record of further disclosures to the educational agency or institution within a reasonable period of time not to exceed 30 days.

(c) The following parties may inspect the record relating to each student:

(1) The parent or eligible student.

(2) The school official or his or her assistants who are responsible for the custody of the records.

(3) Those parties authorized in § 99.31(a) (1) and (3) for the purposes of auditing the recordkeeping procedures of the educational agency or institution.

(d) Paragraph (a) of this section does not apply if the request was from, or the disclosure was to:

(1) The parent or eligible student;

(2) A school official under § 99.31(a)(1);

(3) A party with written consent from the parent or eligible student;

(4) A party seeking directory information; or

(5) A party seeking or receiving records in accordance with § 99.31(a)(9)(ii)(A) through (C).

(Approved by the Office of Management and Budget under control number 1880-0508)

(Authority: 20 U.S.C. 1232g(b)(1) and (b)(4)(A))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74853, Dec. 9, 2008]

§ 99.33 What limitations apply to the redisclosure of information?

(a)

(1) An educational agency or institution may disclose personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.

(2) The officers, employees, and agents of a party that receives information under paragraph (a)(1) of this section may use the information, but only for the purposes for which the disclosure was made.

(b)

(1) Paragraph (a) of this section does not prevent an educational agency or institution from disclosing personally identifiable information with the understanding that the party receiving the information may make further disclosures of the information on behalf of the educational agency or institution if—

(i) The disclosures meet the requirements of § 99.31; and

(ii)

(A) The educational agency or institution has complied with the requirements of § 99.32(b); or

(B) A State or local educational authority or Federal official or agency listed in § 99.31(a)(3) has complied with the requirements of § 99.32(b)(2).

(2) A party that receives a court order or lawfully issued subpoena and rediscloses personally identifiable information from education records on behalf of an educational agency or institution in response to that order or subpoena under § 99.31(a)(9) must provide the notification required under § 99.31(a)(9)(ii).

(c) Paragraph (a) of this section does not apply to disclosures under §§ 99.31(a)(8), (9), (11), (12), (14), (15), and (16), and to information that postsecondary institutions are required to disclose under the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, 20 U.S.C. 1092(f) (Clery Act), to the accuser and accused regarding the outcome of any campus disciplinary proceeding brought alleging a sexual offense.

(d) An educational agency or institution must inform a party to whom disclosure is made of the requirements of paragraph (a) of this section except for disclosures made under §§ 99.31(a)(8), (9), (11), (12), (14), (15), and (16), and to information that postsecondary institutions are required to disclose under the Clery Act to the accuser and accused regarding the outcome of any campus disciplinary proceeding brought alleging a sexual offense.

(Authority: 20 U.S.C. 1232g(b)(4)(B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 65 FR 41853, July 6, 2000; 73 FR 74853, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

§ 99.34 What conditions apply to disclosure of information to other educational agencies or institutions?

(a) An educational agency or institution that discloses an education record under § 99.31(a)(2) shall:

(1) Make a reasonable attempt to notify the parent or eligible student at the last known address of the parent or eligible student, unless:

(i) The disclosure is initiated by the parent or eligible student; or

(ii) The annual notification of the agency or institution under § 99.7 includes a notice that the agency or institution forwards education records to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll or is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer;

(2) Give the parent or eligible student, upon request, a copy of the record that was disclosed; and

(3) Give the parent or eligible student, upon request, an opportunity for a hearing under subpart C.

(b) An educational agency or institution may disclose an education record of a student in attendance to another educational agency or institution if:

(1) The student is enrolled in or receives services from the other agency or institution; and

(2) The disclosure meets the requirements of paragraph (a) of this section.

(Authority: 20 U.S.C. 1232g(b)(1)(B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74854, Dec. 9, 2008]

§ 99.35 What conditions apply to disclosure of information for Federal or State program purposes?

(a)

(1) Authorized representatives of the officials or agencies headed by officials listed in § 99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.

(2) The State or local educational authority or agency headed by an official listed in § 99.31(a)(3) is responsible for using reasonable methods to ensure to the greatest extent practicable that any entity or individual designated as its authorized representative—

(i) Uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs;

(ii) Protects the personally identifiable information from further disclosures or other uses, except as authorized in paragraph (b)(1) of this section; and

(iii) Destroys the personally identifiable information in accordance with the requirements of paragraphs (b) and (c) of this section.

(3) The State or local educational authority or agency headed by an official listed in § 99.31(a)(3) must use a written agreement to designate any authorized representative, other than an employee. The written agreement must—

(i) Designate the individual or entity as an authorized representative;

(ii) Specify—

(A) The personally identifiable information from education records to be disclosed;

(B) That the purpose for which the personally identifiable information from education records is disclosed to the authorized representative is to carry out an audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs; and

(C) A description of the activity with sufficient specificity to make clear that the work falls within the exception of § 99.31(a)(3), including a description of how the personally identifiable information from education records will be used;

(iii) Require the authorized representative to destroy personally identifiable information from education records when the information is no longer needed for the purpose specified;

(iv) Specify the time period in which the information must be destroyed; and

(v) Establish policies and procedures, consistent with the Act and other Federal and State confidentiality and privacy provisions, to protect personally identifiable information from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of personally identifiable information from education records to only authorized representatives with legitimate interests in the audit or evaluation of a Federal- or State-supported education program or for compliance or enforcement of Federal legal requirements related to these programs.

(b) Information that is collected under paragraph (a) of this section must—

(1) Be protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) and their authorized representatives, except that the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of § 99.33(b); and

(2) Be destroyed when no longer needed for the purposes listed in paragraph (a) of this section.

(c) Paragraph (b) of this section does not apply if:

(1) The parent or eligible student has given written consent for the disclosure under § 99.30; or

(2) The collection of personally identifiable information is specifically authorized by Federal law.

(Authority: 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5))

[53 FR 11943, Apr. 11, 1988, as amended at 73 FR 74854, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

§ 99.36 What conditions apply to disclosure of information in health and safety emergencies?

(a) An educational agency or institution may disclose personally identifiable information from an education record to appropriate parties, including parents of an eligible student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals.

(b) Nothing in this Act or this part shall prevent an educational agency or institution from—

(1) Including in the education records of a student appropriate information concerning disciplinary action taken against the student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community;

(2) Disclosing appropriate information maintained under paragraph (b)(1) of this section to teachers and school officials within the agency or institution who the agency or institution has determined have legitimate educational interests in the behavior of the student; or

(3) Disclosing appropriate information maintained under paragraph (b)(1) of this section to teachers and school officials in other schools who have been determined to have legitimate educational interests in the behavior of the student.

(c) In making a determination under paragraph (a) of this section, an educational agency or institution may take into account the totality of the circumstances pertaining to a threat to the health or safety of a student or other individuals. If the educational agency or institution determines that there is an articulable and significant threat to the health or safety of a student or other individuals, it may disclose information

from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. If, based on the information available at the time of the determination, there is a rational basis for the determination, the Department will not substitute its judgment for that of the educational agency or institution in evaluating the circumstances and making its determination.

(Authority: 20 U.S.C. 1232g (b)(1)(I) and (h))

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74854, Dec. 9, 2008]

§ 99.37 What conditions apply to disclosing directory information?

(a) An educational agency or institution may disclose directory information if it has given public notice to parents of students in attendance and eligible students in attendance at the agency or institution of:

(1) The types of personally identifiable information that the agency or institution has designated as directory information;

(2) A parent's or eligible student's right to refuse to let the agency or institution designate any or all of those types of information about the student as directory information; and

(3) The period of time within which a parent or eligible student has to notify the agency or institution in writing that he or she does not want any or all of those types of information about the student designated as directory information.

(b) An educational agency or institution may disclose directory information about former students without complying with the notice and opt out conditions in paragraph (a) of this section. However, the agency or institution must continue to honor any valid request to opt out of the disclosure of directory information made while a student was in attendance unless the student rescinds the opt out request.

(c) A parent or eligible student may not use the right under paragraph (a)(2) of this section to opt out of directory information disclosures to—

(1) Prevent an educational agency or institution from disclosing or requiring a student to disclose the student's name, identifier, or institutional email address in a class in which the student is enrolled; or

(2) Prevent an educational agency or institution from requiring a student to wear, to display publicly, or to disclose a student ID card or badge that exhibits information that may be designated as directory information under § 99.3 and that has been properly designated by the educational agency or institution as directory information in the public notice provided under paragraph (a)(1) of this section.

(d) In its public notice to parents and eligible students in attendance at the agency or institution that is described in paragraph (a) of this section, an educational agency or institution may specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both. When an educational agency or institution specifies that disclosure of directory information will be limited to specific parties, for specific purposes, or both, the educational agency or institution must limit its directory information disclosures to those specified in its public notice that is described in paragraph (a) of this section.

(e) An educational agency or institution may not disclose or confirm directory information without meeting the written consent requirements in § 99.30 if a student's social security number or other non-directory information is used alone or combined with other data elements to identify or help identify the student or the student's records.

(Authority: 20 U.S.C. 1232g(a)(5) (A) and (B))

[53 FR 11943, Apr. 11, 1988, as amended at 73 FR 74854, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

§ 99.38 What conditions apply to disclosure of information as permitted by State statute adopted after November 19, 1974, concerning the juvenile justice system?

(a) If reporting or disclosure allowed by State statute concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records are released, an educational agency or institution may disclose education records under § 99.31(a)(5)(i)(B).

(b) The officials and authorities to whom the records are disclosed shall certify in writing to the educational agency or institution that the information will not be disclosed to any other party, except as provided under State law, without the prior written consent of the parent of the student.

(Authority: 20 U.S.C. 1232g(b)(1)(J))

[61 FR 59297, Nov. 21, 1996]

§ 99.39 What definitions apply to the nonconsensual disclosure of records by postsecondary educational institutions in connection with disciplinary proceedings concerning crimes of violence or non-forcible sex offenses?

As used in this part:

Alleged perpetrator of a crime of violence is a student who is alleged to have committed acts that would, if proven, constitute any of the following offenses or attempts to commit the following offenses that are defined in appendix A to this part:

> Arson
>
> Assault offenses
>
> Burglary
>
> Criminal homicide—manslaughter by negligence
>
> Criminal homicide—murder and nonnegligent manslaughter
>
> Destruction/damage/vandalism of property
>
> Kidnapping/abduction
>
> Robbery

Forcible sex offenses.

Alleged perpetrator of a nonforcible sex offense means a student who is alleged to have committed acts that, if proven, would constitute statutory rape or incest. These offenses are defined in appendix A to this part.

Final results means a decision or determination, made by an honor court or council, committee, commission, or other entity authorized to resolve disciplinary matters within the institution. The disclosure of final results must include only the name of the student, the violation committed, and any sanction imposed by the institution against the student.

Sanction imposed means a description of the disciplinary action taken by the institution, the date of its imposition, and its duration.

Violation committed means the institutional rules or code sections that were violated and any essential findings supporting the institution's conclusion that the violation was committed.

(Authority: 20 U.S.C. 1232g(b)(6))

[65 FR 41853, July 6, 2000]

Subpart E—What Are the Enforcement Procedures?

§ 99.60 What functions has the Secretary delegated to the Office and to the Office of Administrative Law Judges?

(a) For the purposes of this subpart, *Office* means the Office of the Chief Privacy Officer, U.S. Department of Education.

(b) The Secretary designates the Office to:

(1) Investigate, process, and review complaints and violations under the Act and this part; and

(2) Provide technical assistance to ensure compliance with the Act and this part.

(c) The Secretary designates the Office of Administrative Law Judges to act as the Review Board required under the Act to enforce the Act with respect to all applicable programs. The term *applicable program* is defined in section 400 of the General Education Provisions Act.

(Authority: 20 U.S.C. 1232g (f) and (g), 1234)

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 82 FR 6253, Jan. 19, 2017]

§ 99.61 What responsibility does an educational agency or institution, a recipient of Department funds, or a third party outside of an educational agency or institution have concerning conflict with State or local laws?

If an educational agency or institution determines that it cannot comply with the Act or this part due to a conflict with State or local law, it must notify the Office within 45 days, giving the text and citation of the conflicting law. If another recipient of Department funds under any program administered by the Secretary or a third party to which personally identifiable information from education records has been non-consensually disclosed determines that it cannot comply with the Act or this part due to a conflict with State or local law, it also must notify the Office within 45 days, giving the text and citation of the conflicting law.

(Authority: 20 U.S.C. 1232g(f))

[76 FR 75642, Dec. 2, 2011]

§ 99.62 What information must an educational agency or institution or other recipient of Department funds submit to the Office?

The Office may require an educational agency or institution, other recipient of Department funds under any program administered by the Secretary to which personally identifiable information from education records is non-consensually disclosed, or any third party outside of an educational agency or institution to which personally identifiable information from education records is non-consensually disclosed to submit reports, information on policies and procedures, annual notifications, training materials, or other information necessary to carry out the Office's enforcement responsibilities under the Act or this part.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g))

[76 FR 75643, Dec. 2, 2011]

§ 99.63 Where are complaints filed?

A parent or eligible student may file a written complaint with the Office regarding an alleged violation under the Act and this part. The Office's address is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202.

(Authority: 20 U.S.C. 1232g(g))

[65 FR 41854, July 6, 2000, as amended at 73 FR 74854, Dec. 9, 2008]

§ 99.64 What is the investigation procedure?

(a) A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of the Act or this part has occurred. A complaint does not have to allege that a violation is based on a policy or practice of the educational agency or institution, other recipient of Department funds under any program administered by the Secretary, or any third party outside of an educational agency or institution.

(b) The Office investigates a timely complaint filed by a parent or eligible student, or conducts its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether an educational agency or institution or other recipient of Department funds under any program administered by the Secretary has failed to comply with a provision of the Act or this part. If the Office determines that an educational agency or institution or other recipient of Department funds under any program administered by the Secretary has failed to comply with a provision of the Act or this part, it may also determine whether the failure to comply is based on a policy or practice of the agency or institution or other recipient. The Office also investigates a timely complaint filed by a parent or eligible student, or conducts its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether a third party outside of the educational agency or institution has failed to comply with the provisions of § 99.31(a)(6)(iii)(B) or has improperly redisclosed personally identifiable information from education records in violation of § 99.33.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f) and (g))

(c) A timely complaint is defined as an allegation of a violation of the Act that is submitted to the Office within 180 days of the date of the alleged violation or of the date that the complainant knew or reasonably should have known of the alleged violation.

(d) The Office may extend the time limit in this section for good cause shown.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f) and (g))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 65 FR 41854, July 6, 2000; 73 FR 74854, Dec. 9, 2008; 76 FR 75643, Dec. 2, 2011]

§ 99.65 What is the content of the notice of investigation issued by the Office?

(a) The Office notifies in writing the complainant, if any, and the educational agency or institution, the recipient of Department funds under any program administered by the Secretary, or the third party outside of an educational agency or institution if it initiates an investigation under § 99.64(b). The written notice—

(1) Includes the substance of the allegations against the educational agency or institution, other recipient, or third party; and

(2) Directs the agency or institution, other recipient, or third party to submit a written response and other relevant information, as set forth in § 99.62, within a specified period of time, including information about its policies and practices regarding education records.

(b) The Office notifies the complainant if it does not initiate an investigation because the complaint fails to meet the requirements of § 99.64.

(Authority: 20 U.S.C. 1232g(g))

[73 FR 74855, Dec. 9, 2008, as amended at 76 FR 75643, Dec. 2, 2011]

§ 99.66 What are the responsibilities of the Office in the enforcement process?

(a) The Office reviews a complaint, if any, information submitted by the educational agency or institution, other recipient of Department funds under any program administered by the Secretary, or third party outside of an educational agency or institution, and any other relevant information. The Office may permit the parties to submit further written or oral arguments or information.

(b) Following its investigation, the Office provides to the complainant, if any, and the educational agency or institution, other recipient, or third party a written notice of its findings and the basis for its findings.

(c) If the Office finds that an educational agency or institution or other recipient has not complied with a provision of the Act or this part, it may also find that the failure to comply was based on a policy or practice of the agency or institution or other recipient. A notice of findings issued under paragraph (b) of this section to an educational agency or institution, or other recipient that has not complied with a provision of the Act or this part—

(1) Includes a statement of the specific steps that the agency or institution or other recipient must take to comply; and

(2) Provides a reasonable period of time, given all of the circumstances of the case, during which the educational agency or institution or other recipient may comply voluntarily.

(d) If the Office finds that a third party outside of an educational agency or institution has not complied with the provisions of § 99.31(a)(6)(iii)(B) or has improperly redisclosed personally identifiable information from education records in violation of § 99.33, the Office's notice of findings issued under paragraph (b) of this section—

(1) Includes a statement of the specific steps that the third party outside of the educational agency or institution must take to comply; and

(2) Provides a reasonable period of time, given all of the circumstances of the case, during which the third party may comply voluntarily.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g))

[76 FR 75643, Dec. 2, 2011]

§ 99.67 How does the Secretary enforce decisions?

(a) If an educational agency or institution or other recipient of Department funds under any program administered by the Secretary does not comply during the period of time set under § 99.66(c), the Secretary may take any legally available enforcement action in accordance with the Act, including, but not limited to, the following enforcement actions available in accordance with part D of the General Education Provisions Act—

(1) Withhold further payments under any applicable program;

(2) Issue a complaint to compel compliance through a cease and desist order; or

(3) Terminate eligibility to receive funding under any applicable program.

(b) If, after an investigation under § 99.66, the Secretary finds that an educational agency or institution, other recipient, or third party has complied voluntarily with the Act or this part, the Secretary provides the complainant and the agency or institution, other recipient, or third party with written notice of the decision and the basis for the decision.

(c) If the Office finds that a third party, outside the educational agency or institution, violates § 99.31(a)(6)(iii)(B), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation of § 99.31(a)(6)(iii)(B) access to personally identifiable information from education records for at least five years.

(d) If the Office finds that a State or local educational authority, a Federal agency headed by an official listed in § 99.31(a)(3), or an authorized representative of a State or local educational authority or a Federal agency headed by an official listed in § 99.31(a)(3), improperly rediscloses personally identifiable information from education records, then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the improper redisclosure access to personally identifiable information from education records for at least five years.

(e) If the Office finds that a third party, outside the educational agency or institution, improperly rediscloses personally identifiable information from education records in violation of § 99.33 or fails to provide the notification required under § 99.33(b)(2), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation access to personally identifiable information from education records for at least five years.

(Authority: 20 U.S.C. 1232g(b)(4)(B) and (f); 20 U.S.C. 1234c)

[76 FR 75643, Dec. 2, 2011]

Appendix A to Part 99—Crimes of Violence Definitions

Arson

Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle or aircraft, personal property of another, etc.

Assault Offenses

An unlawful attack by one person upon another.

> Note: By definition there can be no "attempted" assaults, only "completed" assaults.

(a) ***Aggravated Assault.*** An unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm. (It is not necessary that injury result from an aggravated assault when a gun, knife, or other weapon is used which could and probably would result in serious injury if the crime were successfully completed.)

(b) ***Simple Assault.*** An unlawful physical attack by one person upon another where neither the offender displays a weapon, nor the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe laceration, or loss of consciousness.

(c) ***Intimidation.*** To unlawfully place another person in reasonable fear of bodily harm through the use of threatening words or other conduct, or both, but without displaying a weapon or subjecting the victim to actual physical attack.

> Note: This offense includes stalking.

Burglary

The unlawful entry into a building or other structure with the intent to commit a felony or a theft.

Criminal Homicide—Manslaughter by Negligence

The killing of another person through gross negligence.

Criminal Homicide—Murder and Nonnegligent Manslaughter

The willful (nonnegligent) killing of one human being by another.

Destruction/Damage/Vandalism of Property

To willfully or maliciously destroy, damage, deface, or otherwise injure real or personal property without the consent of the owner or the person having custody or control of it.

Kidnapping/Abduction

The unlawful seizure, transportation, or detention of a person, or any combination of these actions, against his or her will, or of a minor without the consent of his or her custodial parent(s) or legal guardian.

> Note: Kidnapping/Abduction includes hostage taking.

Robbery

The taking of, or attempting to take, anything of value under confrontational circumstances from the control, custody, or care of a person or persons by force or threat of force or violence or by putting the victim in fear.

> Note: Carjackings are robbery offenses where a motor vehicle is taken through force or threat of force.

Sex Offenses, Forcible

Any sexual act directed against another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent.

(a) ***Forcible Rape*** (Except “Statutory Rape”). The carnal knowledge of a person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her temporary or permanent mental or physical incapacity (or because of his or her youth).

(b) ***Forcible Sodomy.*** Oral or anal sexual intercourse with another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

(c) ***Sexual Assault With An Object.*** To use an object or instrument to unlawfully penetrate, however slightly, the genital or anal opening of the body of another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

Note: An “object” or “instrument” is anything used by the offender other than the offender's genitalia. Examples are a finger, bottle, handgun, stick, etc.

(d) ***Forcible Fondling.*** The touching of the private body parts of another person for the purpose of sexual gratification, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

Note: Forcible Fondling includes “Indecent Liberties” and “Child Molesting.”

Nonforcible Sex Offenses (Except “Prostitution Offenses”)

Unlawful, nonforcible sexual intercourse.

(a) ***Incest.*** Nonforcible sexual intercourse between persons who are related to each other within the degrees wherein marriage is prohibited by law.

(b) ***Statutory Rape.*** Nonforcible sexual intercourse with a person who is under the statutory age of consent.

(Authority: 20 U.S.C. 1232g(b)(6) and 18 U.S.C. 16)

[65 FR 41854, July 6, 2000]

DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary

Director
Office for Civil Rights
Washington, D.C. 20201

December 3, 2025

Re: The HIPAA Privacy Rule and Parental Access to Minor Children's Medical Records

Dear Colleagues:

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services administers and enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, which establish the minimum privacy and security requirements for protected health information (PHI), breach notification requirements that covered entities (health plans, health care clearinghouses, and most health care providers) and their business associates must follow, as well as the rights that individuals (and their personal representatives) have with respect to their PHI, such as the right to access this information.

OCR has become aware that there may be instances in which the parents of minor children are not receiving access to their children's medical records[1] to the extent required by the HIPAA Privacy Rule ("Privacy Rule"). For example, parents, as the personal representative of their minor children, may be denied access to their minor children's medical records, or a covered entity may be requiring minor children to authorize parental access before such access will be granted, when no such requirement exists under applicable law[2] and, thus, under the Privacy Rule. Denial of access in those circumstances may be a violation of the Privacy Rule.

The Privacy Rule establishes the right of an individual, or a personal representative acting on the individual's behalf, to access the individual's medical records and other PHI about the individual.[3] The Privacy Rule provides that, "If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under [the HIPAA Rules], with respect to [PHI] relevant to such personal representation . . . ."[4]

In most cases, a parent is the personal representative of an unemancipated minor child (hereinafter, "child") and can exercise the child's rights with respect to PHI, because the parent usually has the authority to make health care decisions about his or her child. **Accordingly, the Privacy Rule generally gives the parent the right to access the child's medical records as the child's personal representative**, unless one of the limited exceptions applies.

---

[1] Throughout this letter medical records and PHI are used interchangeably.
[2] Applicable law refers to other laws such as state or Tribal law.
[3] The right of access applies to PHI in a designated record set. *See* 45 CFR 164.524.
[4] 45 CFR 164.502(g)(3)(i).

There are three situations in which a child's parent is not a personal representative under the Privacy Rule with respect to some or all of the child's PHI. These exceptions are:

1. **When the child consents to health care and the consent of the parent is not required under state or other applicable law**. In this situation, the parent is not the child's personal representative with respect to PHI related to ***that*** health care.
2. **When the child obtains health care at the direction of a court, or a person appointed by the court**. In this situation, the parent is not the child's personal representative with respect to PHI related to ***that*** health care.
3. **When, and to the extent that, the parent agrees that the child and the health care provider may have a confidential relationship**. In this situation, the scope of the parent's agreement to the confidential relationship determines the degree to which the parent is the child's personal representative for purposes of PHI maintained by that health care provider.

These three exceptions are generally limited to certain types of health care services, such as mental health care. That is, under HIPAA, a parent might be a child's personal representative for—and have the right of access to PHI about—most medical treatments and health care services received by the child, but that parent might not be the child's personal representative with respect to certain limited types of medical treatments and health care services. Whether a parent is their child's personal representative under HIPAA depends, in part, on the laws of the state. Additionally, state law may limit a parent's rights as a child's personal representative, including state-specific limits on the right of a parent to access certain portions of a child's medical records.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may determine not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.[5] This requires an individualized, patient-specific professional determination by the health care provider.

Absent these limited exceptions, where a parent is the personal representative of his or her child, a covered entity (and, where applicable, its business associate acting on the covered entity's behalf) may not place additional limitations on a parent's access to the child's medical records beyond any existing limitations in applicable law.

Consider the following scenarios where, absent the existence of an applicable and specific exception, a parent cannot be denied access to his or her child's PHI:

- A patient is 16 years old, consents to receive treatment for a sexually transmitted infection, and there is a state law that permits children who are 16 years or older to obtain such treatment without parental consent. A covered health care provider might, depending on the particular state law, deny the child's parent access to PHI related to *that* health care. However, the provider may not deny the parent, as the child's personal representative, access to the child's PHI that is unrelated to that particular health care.

[5] *See* 45 CFR 164.502(g)(5).

- A patient is 13 years old, and a state law requires parental consent for patients under 15 years old to receive health care in all cases. A covered health care provider cannot require authorization from that 13-year-old child before the provider will give the parent access to the child's PHI. The covered health care provider could not deny the parent access to that child's health care records by claiming that the 13-year-old child had not authorized parental access.

With respect to electronic access to PHI, covered entities should work with any business associates involved in facilitating such access (*e.g.*, electronic health record or patient portal vendors) to ensure that parents who are their children's personal representatives have electronic access to their children's PHI to the full extent required by the Privacy Rule. This includes establishing electronic access configurations to allow parents access to their children's PHI in accordance with the Privacy Rule. For example, if the default configurations of electronic information systems that maintain a child's PHI result in the improper denial of a parent's right, as the child's personal representative, to timely access the information, the covered entity should modify, or work with their business associate (if applicable) to modify, the default configurations to allow such access as required by the Privacy Rule. A covered entity that denies such access may be in violation of the Privacy Rule.

OCR has the following materials to assist covered entities, business associates, and the public in understanding a personal representative's right to access an individual's medical records and other PHI, particularly in the case of a parent seeking access to their child's medical records.

- Does the HIPAA Privacy Rule Allow Parents the Right to See Their Children's Medical Records?
- HIPAA and Personal Representatives
- Am I My Child's "Personal Representative" Under HIPAA?
- How HIPAA Applies to Mental Health and Substance Use Disorder Information

OCR urges covered entities, and business associates that facilitate the provision of access to PHI on the covered entities' behalf, to review their policies and procedures and, if necessary, proactively make any necessary changes to ensure their compliance with the Privacy Rule. Further, covered entities should ensure that parents' access to their children's medical records in electronic systems (*e.g.*, electronic health records system, patient portal) is properly configured and maintained to provide access in compliance with the Privacy Rule.

Providing parents who are their children's personal representatives with easy access to their children's PHI empowers parents to be more in control of decisions regarding their children's health and well-being. OCR is making parental access to children's medical records an enforcement priority and will use all civil remedies available, including civil money penalties, to ensure compliance with this Privacy Rule requirement.

Sincerely,

/s/

Paula M. Stannard
Director, Office for Civil Rights



Payment Card Industry
Data Security Standard

Requirements and Testing Procedures

Version 4.0.1

June 2024

Document Changes

Date	Version	Description
October 2008	1.2	To introduce PCI DSS v1.2 as "PCI DSS Requirements and Security Assessment Procedures," eliminating redundancy between documents, and making both general and specific changes from PCI DSS Security Audit Procedures v1.1. For complete information, see PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2.
July 2009	1.2.1	Add sentence that was incorrectly deleted between PCI DSS v1.1 and v1.2.
		Correct "then" to "than" in testing procedures 6.3.7.a and 6.3.7.b.
		Remove grayed-out marking for "in place" and "not in place" columns in testing procedure 6.5.b.
		For Compensating Controls Worksheet – Completed Example, correct wording at top of page to say, "Use this worksheet to define compensating controls for any requirement noted as "in place" via compensating controls."
October 2010	2.0	Update and implemented changes from v1.2.1. See PCI DSS – Summary of Changes from PCI DSS Version 1.2.1 to 2.0.
November 2013	3.0	Update from v2.0. See PCI DSS – Summary of Changes from PCI DSS Version 2.0 to 3.0.
April 2015	3.1	Update from PCI DSS v3.0. See PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1 for details of changes.
April 2016	3.2	Update from PCI DSS v3.1. See PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2 for details of changes.
May 2018	3.2.1	Update from PCI DSS v3.2. See PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1 for details of changes.
March 2022	4.0	Rename document title to "Payment Card Industry Data Security Standard: Requirements and Testing Procedures." Update from PCI DSS v3.2.1. See PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0 for details of changes.
June 2024	4.0.1	Update from PCI DSS v4.0. See *PCI DSS - Summary of Changes from PCI DSS Version 4.0 to 4.0.1* for details of changes.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Contents

1 Introduction and PCI Data Security Standard Overview 1

2 PCI DSS Applicability Information 4

3 Relationship between PCI DSS and PCI SSC Software Standards 7

4 Scope of PCI DSS Requirements 9

5 Best Practices for Implementing PCI DSS into Business-as-Usual Processes 19

6 For Assessors: Sampling for PCI DSS Assessments 22

7 Description of Timeframes Used in PCI DSS Requirements 25

8 Approaches for Implementing and Validating PCI DSS 28

9 Protecting Information About an Entity's Security Posture 30

10 Testing Methods for PCI DSS Requirements 31

11 Instructions and Content for Report on Compliance 32

12 PCI DSS Assessment Process 33

13 Additional References 34

14 PCI DSS Versions 35

15 Detailed PCI DSS Requirements and Testing Procedures 36

Build and Maintain a Secure Network and Systems 38

Requirement 1: Install and Maintain Network Security Controls 38

Requirement 2: Apply Secure Configurations to All System Components 61

Protect Account Data 74

Requirement 3: Protect Stored Account Data 74

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks 110

Maintain a Vulnerability Management Program 119

Requirement 5: Protect All Systems and Networks from Malicious Software 119

Requirement 6: Develop and Maintain Secure Systems and Software 134

Implement Strong Access Control Measures 161

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know 161

Requirement 8: Identify Users and Authenticate Access to System Components 174

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9: Restrict Physical Access to Cardholder Data *210*
Regularly Monitor and Test Networks 236
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data *236*
Requirement 11: Test Security of Systems and Networks Regularly *260*
Maintain an Information Security Policy 290
Requirement 12: Support Information Security with Organizational Policies and Programs *290*

Appendix A Additional PCI DSS Requirements **334**

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers *335*
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections *342*
Appendix A3: Designated Entities Supplemental Validation (DESV) *346*

Appendix B Compensating Controls **369**

Appendix C Compensating Controls Worksheet **371**

Appendix D Customized Approach **372**

Appendix E Sample Templates to Support Customized Approach **374**

Appendix F Leveraging the PCI Software Security Framework to Support Requirement 6 ..... **375**

Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms **379**

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

1 Introduction and PCI Data Security Standard Overview

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

Table 1 shows the 12 principal PCI DSS requirements.

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

This document, the Payment Card Industry Data Security Standard Requirements and Testing Procedures, consists of the 12 PCI DSS principal requirements, detailed security requirements, corresponding testing procedures, and other information pertinent to each requirement. The following sections provide detailed guidelines and best practices to assist entities to prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS requirements and testing procedures begin on page 43.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, and to incorporate local, regional, and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name).

Limitations

If any of the requirements contained in this standard conflict with country, state, or local laws, the country, state, or local law will apply.

PCI DSS Resources

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) provides the following additional resources to assist organizations with their PCI DSS assessments and validations:

- Document Library, including:
  - PCI DSS Summary of Changes
  - PCI DSS Quick Reference Guide
  - Information Supplements and Guidelines
  - Prioritized Approach for PCI DSS
  - Report on Compliance (ROC) Reporting Template and Reporting Instructions
  - Self-Assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines
  - Attestations of Compliance *(*AOCs*)*
- Frequently Asked Questions (FAQs)
- PCI for Small Merchants website
- PCI training courses and informational webinars
- List of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- Lists of PCI approved devices, applications, and solutions

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

There are over 60 guidance documents and information supplements available on the PCI SSC website that provide specific guidance and considerations for PCI DSS. Examples include:

- Guidance for PCI DSS Scoping and Network Segmentation
- PCI SSC Cloud Computing Guidelines
- Multi-Factor Authentication Guidance
- Third-Party Security Assurance
- Effective Daily Log Monitoring
- Penetration Testing Guidance
- Best Practices for Implementing a Security Awareness Program
- Best Practices for Maintaining PCI DSS Compliance
- PCI DSS for Large Organizations
- Use of SSL/Early TLS and Impact on ASV Scans
- Use of SSL/Early TLS for POS POI Terminal Connections
- Tokenization Product Security Guidelines
- Protecting Telephone-Based Payment Card Data

Note: *Information Supplements complement PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements. Information Supplements do not supersede, replace, or extend PCI DSS or any of its requirements.*

Refer to the Document Library at www.pcisecuritystandards.org for information about these and other resources.

In addition, refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

2 PCI DSS Applicability Information

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data and/or sensitive authentication data. This includes all entities involved in payment account processing —including merchants, processors, acquirers, issuers, and other service providers.

Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers); contact these organizations for any additional criteria.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of cardholder data and/or sensitive authentication data. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data—for example, entities that outsource payment operations or management of their cardholder data environment (CDE)[1]. Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

[1] In accordance with those organizations that manage compliance programs (such as payment brands and acquirers); entities should contact these organizations for more details.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

The primary account number (PAN) is the defining factor for cardholder data. The term account data therefore covers the following: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data.

If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the CDE, they must be protected in accordance with the PCI DSS requirements applicable to cardholder data.

If an entity stores, processes, or transmits PAN, then a CDE exists to which PCI DSS requirements will apply. Some requirements may not be applicable, for example if the entity does not store PAN, then the requirements relating to the protection of stored PAN in Requirement 3 will not be applicable to the entity.

Even if an entity does not store, process, or transmit PAN, some PCI DSS requirements may still apply. Consider the following:

- If the entity stores SAD, requirements specifically related to SAD storage in Requirement 3 will be applicable.
- If the entity engages third-party service providers to store, process or transmit PAN on its behalf, requirements related to the management of service providers in Requirement 12 will be applicable.
- If the entity can impact the security of cardholder data and/or sensitive authentication data because the security of an entity's infrastructure can affect how cardholder data is processed (for example, via a web server that controls the generation of a payment form or page) some requirements will be applicable.
- If cardholder data is only present on physical media (for example paper), requirements relating to the security and disposal of physical media in Requirement 9 will be applicable.
- Requirements related to an incident response plan are applicable to all entities, to ensure that there are procedures to follow in the event of a suspected or actual breach of the confidentiality of cardholder data.

Use of Account Data, Sensitive Authentication Data, Cardholder Data, and Primary Account Number in PCI DSS

PCI DSS includes requirements that specifically refer to account data, cardholder data, and sensitive authentication data. It is important to note that each of these types of data are different and the terms are not interchangeable. Specific references within requirements to account data, cardholder data, or sensitive authentication data are purposeful, and the requirements apply specifically to the type of data that is referenced.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Elements of Account Data and Storage Requirements

Table 3 identifies the elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be rendered unreadable—for example, with strong cryptography—when stored. This table is not exhaustive and is presented to illustrate only how the stated requirements apply to the different data elements.

Table 3. Account Data Element Storage Requirements

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
		Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2 [2]	No
		Service Code		
		Expiration Date		
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization as defined in Requirement 3.3.1 [3]	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
		Card verification code		
		PIN/PIN Block		

If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.5.1.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even for environments where there is no PAN present.

[2] Where data exists in the same environment as PAN.
[3] Except as permitted for issuers and companies that support issuing services. Requirements for issuers and issuing services are separately defined in Requirement 3.3.3.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

3 Relationship between PCI DSS and PCI SSC Software Standards

PCI SSC supports the use of secure payment software within cardholder data environments (CDE) via the Software Security Framework (SSF), which consists of the Secure Software Standard and the Secure Software Lifecycle (Secure SLC) Standard. Software that is PCI SSC validated and listed provides assurance that the software has been developed using secure practices and has met a defined set of software security requirements.

The PCI SSC secure software programs include listings of payment software and software vendors that have been validated as meeting the applicable PCI SSC Software Standards.

- **Validated Software**: Payment software listed on the PCI SSC website as a Validated Payment Application (PA-DSS) or Validated Payment Software (the Secure Software Standard) has been evaluated by a qualified assessor to confirm the software meets the security requirements within that standard. The security requirements in these standards are focused on protecting the integrity and confidentiality of payment transactions and account data.
- **Qualified Software Vendors**: The Secure SLC Standard defines security requirements for software vendors to integrate secure software development practices throughout the entire software lifecycle. Software vendors that have been validated as meeting the Secure SLC Standard are listed on the PCI SSC website as a Secure SLC Qualified Vendor.

Note: *PA-DSS and the related program were retired in October 2022. Refer to the PCI SSC List of Validated Payment Applications for expiry dates for PA-DSS validated applications. Since the expiry date, applications are listed as "Acceptable only for Pre-Existing Deployments." Whether an entity can continue to use a PA-DSS application with an expired listing is at the discretion of organizations that manage compliance programs (such as payment brands and acquirers); entities should contact these organizations for more details.*

For more information about the SSF or PA-DSS, refer to the respective Program Guides at www.pcisecuritystandards.org.

All software that stores, processes, or transmits account data, or that could impact the security of cardholder data and/or sensitive authentication data, is in scope for an entity's PCI DSS assessment. While the use of validated payment software supports the security of an entity's CDE, the use of such software does not by itself make an entity PCI DSS compliant. The entity's PCI DSS assessment should include verification that the software is properly configured and securely implemented to support applicable PCI DSS requirements. Additionally, if PCI-listed payment software has been customized, a more in-depth review will be required during the PCI DSS assessment because the software may no longer be representative of the version that was originally validated.

Because security threats are constantly evolving, software that is no longer supported by the vendor (for example, identified by the vendor as "end of life") may not offer the same level of security as supported versions. Entities are strongly encouraged to keep their software current and updated to the latest software versions available.

Entities that develop their own software are encouraged to refer to PCI SSC's software security standards and consider the requirements therein as best practices to use in their development environments. Secure payment software implemented in a PCI DSS compliant environment will help minimize the potential for security breaches leading to compromises of account data and fraud. See *Bespoke and Custom Software*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Applicability of PCI DSS to Payment Software Vendors

PCI DSS may apply to a payment software vendor if the vendor is also a service provider that stores, processes, or transmits account data, or has access to their customers' account data—for example, in the role of a payment service provider or via remote access to a customer environment. Software vendors to which PCI DSS may be applicable include those offering payment services, as well as cloud service providers offering payment terminals in the cloud, software as a service (SaaS), e-commerce in the cloud, and other cloud payment services.

Bespoke and Custom Software

All bespoke and custom software that stores, processes, or transmits account data, or that could impact the security of cardholder data and/or sensitive authentication data, is in scope for an entity's PCI DSS assessment.

Bespoke and custom software that has been developed and maintained in accordance with one of PCI SSC's Software Security Framework standards (the Secure Software Standard or the Secure SLC standard) will support an entity in meeting PCI DSS Requirement 6.

See Appendix F for more details.

Note: *PCI DSS Requirement 6 fully applies to bespoke and custom software that has not been developed and maintained in accordance with one of PCI SSC's Software Security Framework standards. Entities that use software vendors to develop bespoke or custom software that could impact the security of their cardholder data and/or sensitive authentication data are responsible for ensuring those software vendors develop the software according to PCI DSS Requirement 6.*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

4 Scope of PCI DSS Requirements

PCI DSS requirements apply to:

- The cardholder data environment (CDE), which is comprised of:
  - System components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and,
  - System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

AND

- System components, people, and processes that could impact the security of cardholder data and/or sensitive authentication data. [4]

"System components" include network devices, servers, computing devices, virtual components, cloud components, and software. Examples of system components include but are not limited to:

- Systems that store, process, or transmit account data (for example, payment terminals, authorization systems, clearing systems, payment middleware systems, payment back-office systems, shopping cart and store front systems, payment gateway/switch systems, fraud monitoring systems).
- Systems that provide security services (for example, authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems (for example, badge access or CCTV), multi-factor authentication systems, anti-malware systems).
- Systems that facilitate segmentation (for example, internal network security controls).
- Systems that could impact the security of account data or the CDE (for example, name resolution, or e-commerce (web) redirection servers).
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, CDEs residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools.

[4] For additional guidance, refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* on the PCI SSC website.

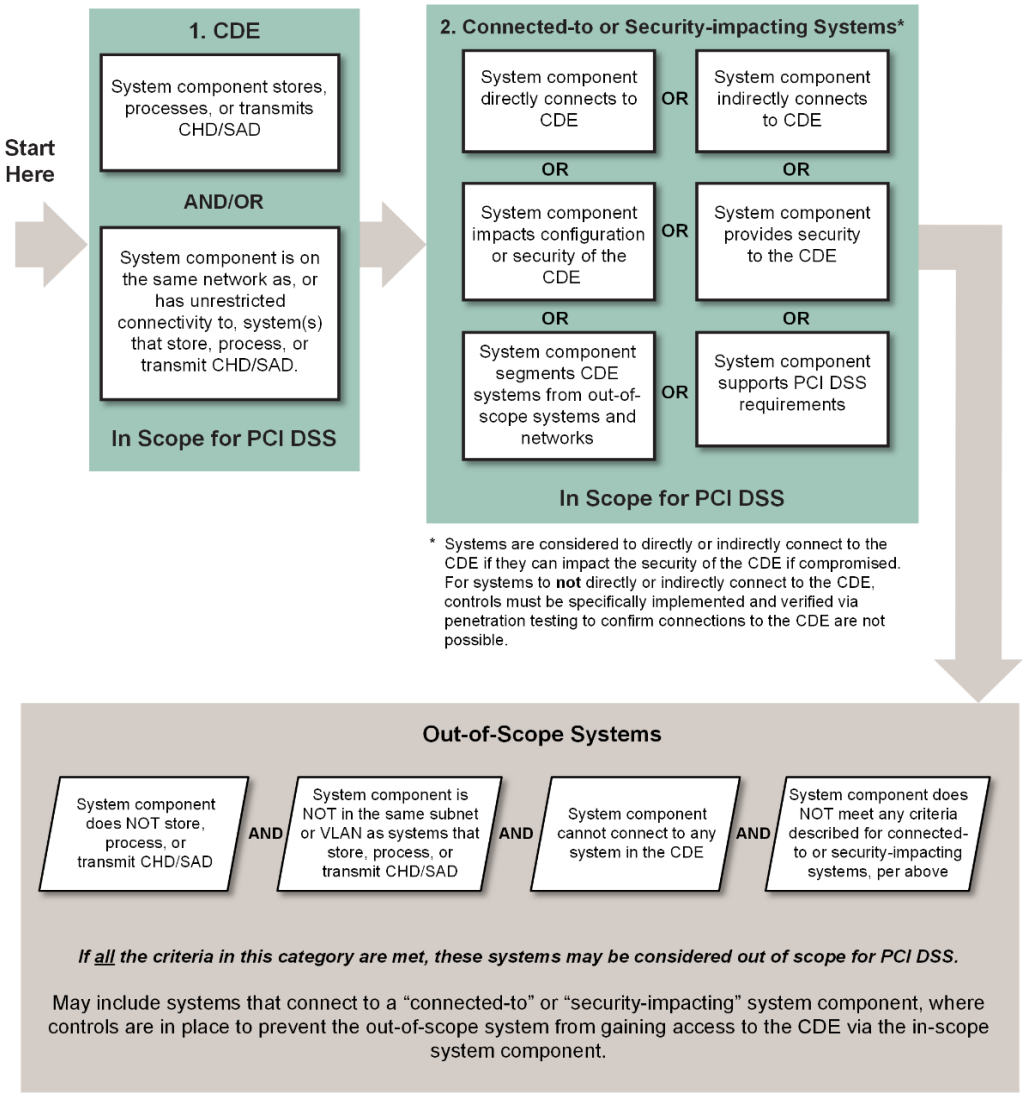
©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

- Network components, including but not limited to network security controls, switches, routers, VoIP network devices, wireless access points, network appliances, and other security appliances.
- Server types, including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices.
- Printers, and multi-function devices that scan, print, and fax.
- Storage of account data in any format (for example, paper, data files, audio files, images, and video recordings).
- Applications, software, and software components, serverless applications, including all purchased, subscribed (for example, Software-as-a-Service), bespoke and custom software, including internal and external (for example, Internet) applications.
- Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the CDE or to systems that can impact the CDE.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Figure 1 shows considerations for scoping system components for PCI DSS.

Figure 1. Understanding PCI DSS Scoping



©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Annual PCI DSS Scope Confirmation

The first step in preparing for a PCI DSS assessment is for the entity to accurately determine the scope of the review. The assessed entity must confirm the accuracy of their PCI DSS scope according to PCI DSS Requirement 12.5.2 by identifying all locations and flows of account data, and identifying all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers, remote access servers, logging servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered during the scoping process, including backup/recovery sites and fail-over systems.

The minimum steps for an entity to confirm the accuracy of their PCI DSS scope are specified in PCI DSS Requirement 12.5.2. The entity is expected to retain documentation to show how PCI DSS scope was determined. The documentation is retained for assessor review and for reference during the entity's next PCI DSS scope confirmation activity. For each PCI DSS assessment, the assessor validates that the entity accurately defined and documented the scope of the assessment.

***Note**: This annual confirmation of PCI DSS scope is defined at PCI DSS Requirement at 12.5.2 and is an activity expected to be performed by the entity. This activity is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the assessment.*

Segmentation

Segmentation (or isolation) of the CDE from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce the:

- Scope of the PCI DSS assessment
- Cost of the PCI DSS assessment
- Cost and difficulty of implementing and maintaining PCI DSS controls
- Risk to an organization relative to payment account data (reduced by consolidating that data into fewer, more controlled locations)

Without adequate segmentation (sometimes called a "flat network"), the entire network is in scope for the PCI DSS assessment. Segmentation can be achieved using a number of physical or logical methods, such as properly configured internal network security controls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network. To be considered out of scope for PCI DSS, a system component must be properly segmented (isolated) from the CDE, such that the out-of-scope system component could not impact the security of cardholder data and/or sensitive authentication data, even if that component was compromised.

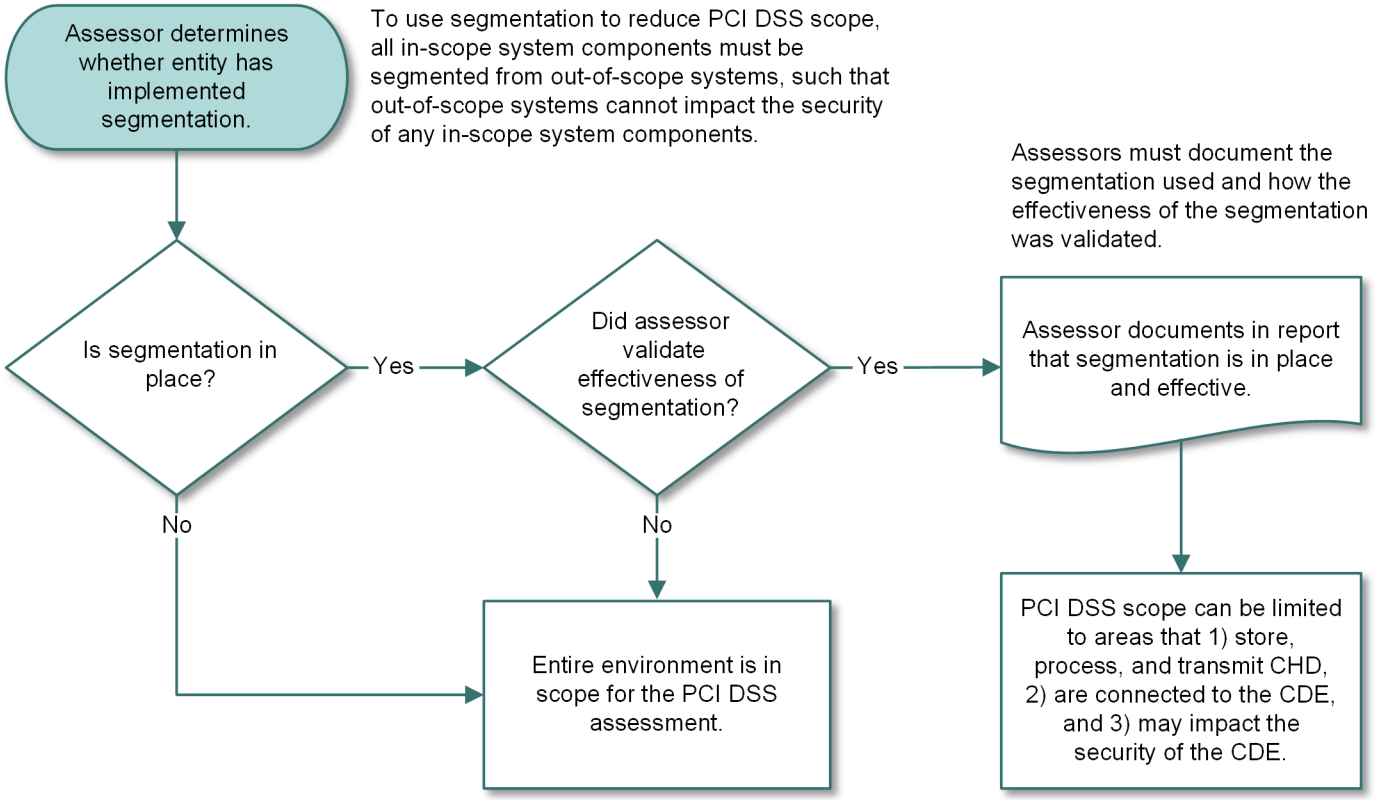
An important prerequisite to reduce the scope of the CDE is a clear understanding of business needs and processes related to the storage, processing, and transmission of account data. Restricting account data to as few locations as possible by eliminating unnecessary data and consolidating necessary data may require reengineering of long-standing business practices.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Documenting account data flows via a data-flow diagram helps an entity fully understand how account data comes into an organization, where it resides within the organization, and how it traverses through various systems within the organization. Data-flow diagrams also illustrate all locations where account data is stored, processed, and transmitted. This information supports an entity implementing segmentation and can also support confirming that segmentation is being used to isolate the CDE from out-of-scope networks.

If segmentation is used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment, as illustrated in Figure 2. At a high level, adequate segmentation isolates systems that store, process, or transmit account data from those that do not. However, the adequacy of a specific segmentation implementation is highly variable and depends on several factors such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Figure 2. Segmentation and Impact to PCI DSS Scope



©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Wireless

If wireless technology is used to store, process, or transmit account data (for example, wireless point-of-sale devices), or if a wireless local area network (WLAN) is part of or connected to the CDE, the PCI DSS requirements and testing procedures for securing wireless environments apply and must be performed.

Rogue wireless detection must be performed per PCI DSS Requirement 11.2.1 even when wireless is not used within the CDE and the entity has a policy that prohibits the use of wireless technology within its environment. This is because of the ease with which a wireless access point can be attached to a network, the difficulty in detecting its presence, and the increased risk presented by unauthorized wireless devices.

Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

When Cardholder Data and/or Sensitive Authentication Data is Accidentally Received via an Unintended Channel

There could be occurrences where an entity receives cardholder data and/or sensitive authentication data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either:

- Include the channel in the scope of their CDE and secure it according to PCI DSS

Or

- Securely delete the data and implement measures to prevent the channel from being used in the future for sending such data.

Encrypted Cardholder Data and Impact on PCI DSS Scope

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable according to PCI DSS Requirement 3.5. However, encryption alone is generally insufficient to render the cardholder data out of scope for PCI DSS and does not remove the need for PCI DSS in that environment. The entity's environment is still in scope for PCI DSS due to the presence of cardholder data. For example, for a merchant card-present environment, there is physical access to the payment cards to complete a transaction and there may also be paper reports or receipts with cardholder data. Similarly, in merchant card-not-present environments, such as mail-order/telephone-order and e-commerce, payment card details are provided via channels that need to be evaluated and protected according to PCI DSS.

The following are each in scope for PCI DSS:

- Systems performing encryption and/or decryption of cardholder data, and systems performing key management functions,
- Encrypted cardholder data that is not isolated from the encryption and decryption and key management processes,

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

- Encrypted cardholder data that is present on a system or media that also contains the decryption key,
- Encrypted cardholder data that is present in the same environment as the decryption key,
- Encrypted cardholder data that is accessible to an entity that also has access to the decryption key.

***Note**: A PCI-listed P2PE solution can significantly reduce the number of PCI DSS requirements applicable to a merchant's cardholder data environment. However, it does not completely remove the applicability of PCI DSS in the merchant environment.*

Encrypted Cardholder Data and Impact to PCI DSS Scope for Third-Party Service Providers

Where a third-party service provider (TPSP) receives and/or stores only data encrypted by another entity, and where they do not have the ability to decrypt the data, the TPSP may be able to consider the encrypted data out of scope if certain conditions are met. This is because responsibility for the data generally remains with the entity, or entities, with the ability to decrypt the data or impact the security of the encrypted data. Determining which party is responsible for specific PCI DSS controls will depend on several factors, including who has access to the decryption keys, the role performed by each party, and the agreement between parties. Responsibilities should be clearly defined and documented to ensure both the TPSP and the entity providing the encrypted data understand which entity is responsible for which security controls.

As an example, a TPSP providing storage services receives and stores encrypted cardholder data provided by customers for back-up purposes. This TPSP does not have access to the encryption or decryption keys, nor does it perform any key management for its customers. The TPSP can exclude any such encrypted data when determining its PCI DSS scope. However, the TPSP does maintain responsibility for controlling access to the encrypted data storage as part of its service agreements with its customers.

Responsibility for ensuring that the encrypted data and the cryptographic keys are protected according to applicable PCI DSS requirements is often shared between entities. In the above example, the customer determines which of their personnel are authorized to access the storage media, and the storage facility is responsible for managing the physical and/or logical access controls to ensure that only persons authorized by the customer are granted access to the storage media. The specific PCI DSS requirements applicable to a TPSP will depend on the services provided and the agreement between the two parties. In the example of a TPSP providing storage services, the physical and logical access controls provided by the TPSP will need to be reviewed at least annually. This review could be performed as part of the merchant's PCI DSS assessment or, alternatively, the review could be performed, and controls validated, by the TPSP with appropriate evidence provided to the merchant. For information about "appropriate evidence," see *Options for TPSPs to Validate PCI DSS Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.*

As another example, a TPSP that receives only encrypted cardholder data for the purposes of routing to other entities, and that does not have access to the data or cryptographic keys, may not have any PCI DSS responsibility for that encrypted data. In this scenario, where the TPSP is not providing any security services or access controls, they may be considered the same as a public or untrusted network, and it would be the responsibility of the entity(s) sending/receiving account data through the TPSP's network to ensure PCI DSS controls are applied to protect the data being transmitted.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Use of Third-Party Service Providers

An entity (referred to as the "customer" in this section) might choose to use a third-party service provider (TPSP) to store, process, or transmit account data or to manage in-scope system components on the customer's behalf. Use of a TPSP may have an impact on the security of a customer's CDE.

***Note**: Use of a PCI DSS compliant TPSP does not make a customer PCI DSS compliant, nor does it remove the customer's responsibility for its own PCI DSS compliance. Even if a customer uses a TPSP, that customer remains responsible for confirming its own compliance as requested by organizations that manage compliance programs (for example, payment brands and acquirers). Customers should contact these organizations for any requirements.*

Using TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8

There are many different scenarios where a customer might use one or more TPSPs for functions within or related to the customer's CDE. In all scenarios where a TPSP is used, the customer must manage and oversee all their TPSP relationships and monitor the PCI DSS compliance status of their TPSPs in accordance with Requirement 12.8, including TPSPs that:

- Have access to the customer's CDE,
- Manage in-scope system components on the customer's behalf, and/or
- Can impact the security of the customer's cardholder data and/or sensitive authentication data.

Managing TPSP relationships in accordance with Requirement 12.8 includes performing due diligence, having appropriate agreements in place, identifying which requirements apply to the customer and which apply to the TPSP, and monitoring the compliance status of TPSPs at least annually.

Requirement 12.8 does not specify that the customer's TPSPs must be PCI DSS compliant, only that the customer monitors their compliance status as specified in the requirement. Therefore, a TPSP does not need to be PCI DSS compliant for its customer to meet Requirement 12.8.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements

When the TPSP provides a service that meets a PCI DSS requirement(s) on the customer's behalf or where that service may impact the security of the customer's cardholder data and/or sensitive authentication data, then those requirements are in scope for the customer's assessment and the compliance of that service will impact the customer's PCI DSS compliance. The TPSP must demonstrate it meets applicable PCI DSS requirements for those requirements to be in place for its customers. For example, if an entity engages a TPSP to manage its network security controls, and the TPSP does not provide evidence that it meets the applicable requirements in PCI DSS Requirement 1, then those requirements are not in place for the customer's assessment. As another example, TPSPs that store backups of cardholder data on behalf of customers would need to meet the applicable requirements related to access controls, physical security, etc., for their customers to consider those requirements in place for their assessments.

Importance of Understanding Responsibilities Between TPSP Customers and TPSPs

When a TPSP provides a service that meets a PCI DSS requirement(s) on the customer's behalf or where that service may impact the security of the customer's cardholder data and/or sensitive authentication data, it is important that customers and TPSPs clearly identify and understand the following:

- The services and system components included in the scope of the TPSP's PCI DSS assessment,
- The specific PCI DSS requirements and sub-requirements covered by the TPSP's PCI DSS assessment,
- Any requirements that are the responsibility of the TPSP's customers to include in their own PCI DSS assessments, and
- Any PCI DSS requirements for which the responsibility is shared between the TPSP and its customers.

For example, a cloud provider should clearly define which of its IP addresses are scanned as part of its quarterly vulnerability scan process and which IP addresses are their customers' responsibility to scan.

Per Requirement 12.9.2, TPSPs are required to support their customers' requests for information about the TPSP's PCI DSS compliance status related to the services provided to customers, and about which PCI DSS requirements are the responsibility of the TPSP, which are the responsibility of the customer, and any responsibilities shared between the customer and the TPSP. Refer to *Information Supplement: Third-Party Security Assurance* for a sample responsibility matrix template that may be used for documenting and clarifying how responsibilities are shared between TPSPs and customers.

Note that not all TPSP relationships require that TPSPs provide customers with documentation of how responsibilities are shared between TPSPs and customers. TPSPs are only required to share such documentation if that TPSP is meeting a PCI DSS requirement(s) on the customer's behalf, if responsibility for meeting a PCI DSS requirement is shared between the TPSP and its customer, or if the TPSP's service may impact the security of the customer's cardholder data and/or sensitive authentication data. While a TPSP may not be required to provide its customers with such documentation because there are no shared responsibilities, the TPSP still needs to support customers by providing their PCI DSS compliance status information, so that customers can manage and monitor their TPSPs in accordance with PCI DSS Requirement 12.8.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Options for TPSPs to Validate PCI DSS Compliance for TPSP Services that Meet Customers' PCI DSS Requirements

TPSPs are responsible for demonstrating their PCI DSS compliance as requested by organizations that manage compliance programs (for example, payment brands and acquirers). TPSPs should contact these organizations for any requirements.

When a TPSP provides services that are intended to meet or facilitate meeting a customer's PCI DSS requirements or that may impact the security of a customer's cardholder data and/or sensitive authentication data, these requirements are in scope for the customer's PCI DSS assessments. There are two options for TPSPs to validate compliance in this scenario:

- **Annual assessment**: TPSP undergoes an annual PCI DSS assessment(s) and provides evidence to its customers to show the TPSP meets the applicable PCI DSS requirements; or
- **Multiple, on-demand assessments**: If a TPSP does not undergo an annual PCI DSS assessment, it must undergo assessments upon request of their customers and/or participate in each of its customers' PCI DSS assessments, with the results of each review provided to the respective customer(s).

If the TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer, and that the relevant PCI DSS requirements were examined and determined to be in place. If the provider has an PCI DSS Attestation of Compliance (AOC), it is expected that the TPSP provides the AOC to customers upon request. The customer may also request relevant sections of the TPSP's PCI DSS Report on Compliance (ROC). The ROC may be redacted to protect any confidential information.

If the TPSP does not undergo its own PCI DSS assessment and therefore does not have an AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that the customer (or its assessor) is able to confirm that the TPSP is meeting those PCI DSS requirements.

TPSP's Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers

For a customer that is monitoring a TPSP's compliance status in accordance with Requirement 12.8, the TPSP's presence on a payment brand's list of PCI DSS compliant service providers ***may be sufficient evidence*** of the TPSP's compliance status if it is clear from the list that the services applicable to the customer were covered by the TPSP's PCI DSS assessment. If it is not clear from the list, the customer should obtain other written confirmation that addresses the TPSP's PCI DSS compliance status.

For a customer that is looking for evidence of PCI DSS compliance for requirements that a TPSP meets on a customer's behalf or where the service provided can impact the security of the customer's cardholder data and/or sensitive authentication data, the TPSP's presence on a payment brand's list of PCI DSS compliant service providers ***is not sufficient evidence*** that the applicable PCI DSS requirements for that TPSP were included in the assessment. If the TPSP has an PCI DSS AOC, it is expected to provide it to customers upon request.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

5 Best Practices for Implementing PCI DSS into Business-as-Usual Processes

An entity that implements business-as-usual processes, otherwise known as BAU, as part of their overall security strategy is taking measures to ensure that the security controls implemented to secure data and an environment continue to be implemented correctly and functioning properly as normal course of business.

Some PCI DSS requirements are intended to act as BAU processes by monitoring security controls to ensure their effectiveness on an ongoing basis. This oversight by the entity assists with providing reasonable assurance that the compliance of its environment is preserved between PCI DSS assessments. While there are currently some BAU requirements defined within the standard, an entity should adopt additional BAU processes specific to their organization and environment when possible. BAU processes are a way to verify that automated and manual controls are performing as expected. Regardless of whether a PCI DSS requirement is automated or manual, it is important for BAU processes to detect anomalies, and alert and report so that responsible individuals address the situation in a timely manner.

Examples of how PCI DSS should be incorporated into BAU activities include, but are not limited to:

- Assigning overall responsibility and accountability for PCI DSS compliance to an individual or team. This can include a charter defined by executive management for a specific PCI DSS compliance program and communication to executive management.
- Developing performance metrics to measure the effectiveness of security initiatives and continuous monitoring of security controls, including those that are heavily relied upon, such as network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), change-detection mechanisms, anti-malware solutions, and access controls, to ensure they are operating effectively and as intended.
- Reviewing logged data more frequently to gain insights to trends or behaviors that may not be obvious with only monitoring.
- Ensuring that all failures in security controls are detected and responded to promptly. Processes to respond to security control failures should include:
  - Restoring the security control.
  - Identifying the cause of failure.
  - Identifying and addressing any security issues that arose during the failure of the security control.
  - Implementing mitigation, such as process or technical controls, to prevent the cause of the failure from recurring.
  - Resuming monitoring of the security control, perhaps with enhanced monitoring for a period of time, to verify the control is operating effectively.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

- Reviewing changes that could introduce security risks to the environment (for example, addition of new systems, changes in system or network configurations) prior to completing the change, and including the following:
  - Perform a risk assessment to determine the potential impact to PCI DSS scope (for example, a new network security control rule that permits connectivity between a system in the CDE and another system could bring additional systems or networks into scope for PCI DSS).
  - Identify PCI DSS requirements applicable to systems and networks affected by the changes (for example, if a new system is in scope for PCI DSS, it would need to be configured per system configuration standards, including change-detection mechanisms, anti-malware software, patches, and audit logging. These new systems and networks would need to be added to the inventory of in-scope system components and to the quarterly vulnerability scan schedule).
  - Update PCI DSS scope and implement security controls as appropriate.
  - Update documentation to reflect implemented changes.
- Reviewing the impact to PCI DSS scope and requirements upon changes to organizational structure (for example, a company merger or acquisition).
- Reviewing external connections and third-party access periodically.
- For entities that use third parties for software development, periodically confirming that those software development activities continue to comply with software development requirements in Requirement 6.
- Performing periodic reviews to confirm that PCI DSS requirements continue to be in place and personnel follow established processes. Periodic reviews should cover all facilities and locations, including retail outlets and data centers, whether self-managed or if a TPSP is used. For example, periodic reviews can be used to confirm that configuration standards have been applied to applicable systems, default vendor accounts and passwords are removed or disabled, patches and anti-malware solutions are up to date, audit logs are being reviewed, and so on. The frequency of periodic reviews should be determined by the entity as appropriate for the size and complexity of their environment, if not otherwise stated in PCI DSS.

These reviews can also be used to verify that required evidence for a PCI DSS assessment is being maintained. For example, evidence of audit logs, vulnerability scan reports, and reviews of network security control rulesets are necessary to assist the entity in preparing for its next PCI DSS assessment.

- Establishing communication with all impacted parties, both external and internal, about newly identified threats and changes to the organization structure. Communication materials should help recipients understand the impact of threats, mitigating steps, and contact points for further information or escalation.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

- Reviewing hardware and software technologies at least once every 12 months to confirm that they continue to be supported by the vendor and can meet the entity's security requirements, including PCI DSS. If technologies are no longer supported by the vendor or cannot meet the entity's security needs, the entity should prepare a remediation plan, including replacement of the technology, as necessary.

***Note**: Some best practices in this section are also included as PCI DSS requirements for certain entities. For example, those undergoing a full PCI DSS assessment, service providers validating to the additional "service provider only" requirements, and designated entities that are required to validate according to Appendix A3: Designated Entities Supplemental Validation.*

Each entity should consider implementing these best practices into their environment, even if the entity is not required to validate to them (for example, merchants undergoing self-assessment).

Refer to *Best Practices for Maintaining PCI DSS Compliance* in the Document Library on the PCI SSC website for additional guidance.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

6 For Assessors: Sampling for PCI DSS Assessments

Sampling is an option for assessors conducting PCI DSS assessments to facilitate the assessment process when there are large numbers of items in a population being tested.

While it is acceptable for an assessor to sample from similar items in a population being tested as part of its review of an entity's PCI DSS compliance, it is not acceptable for an entity to apply PCI DSS requirements to only a sample of its environment (for example, requirements for quarterly vulnerability scans apply to all system components). Similarly, it is not acceptable for an assessor to review only a sample of PCI DSS requirements for compliance.

While sampling allows assessors to test less than 100% of a given sampling population, assessors should always strive for the most complete review possible. Assessors are encouraged to use automated processes or other mechanisms if the complete population, regardless of size, can be tested quickly and efficiently with minimal impact on the resources of the entity being assessed. Where automated processes are not available to test 100% of a population, sampling is an equally acceptable approach.

After considering the overall scope, complexity, and consistency of the environment being assessed, and the nature (automated or manual) of the processes used by an entity to meet a requirement, the assessor may independently select representative samples from the populations being reviewed in order to assess the entity's compliance with PCI DSS requirements. Samples must be a representative selection of all variants of the population and must be sufficiently large to provide the assessor with assurance that controls are implemented as expected across the entire population. Where testing the periodic performance of a requirement (for example, weekly or quarterly, or periodically), the assessor should attempt to select a sample that represents the entire period covered by the assessment so that the assessor may make a reasonable judgment that the requirement was met throughout the assessment period. Testing the same sample of items year after year could allow unknown variations in the non-sampled items to remain undetected. Assessors must revalidate the sampling rationale for each assessment and consider previous sample sets. Different samples must be selected for each assessment.

Appropriate selection of the sample depends on what is being considered in examining the sample members. For example, determining the presence of anti-malware on servers known to be affected by malicious software may lead to determining the population to be all servers in the environment, or all servers in the environment that are running a particular operating system, or all servers that are not mainframes, etc. Selection of an appropriate sample would then include representatives of ALL members of the identified population, including all servers running the identified operating system including all versions, as well as servers within the population that are used for different functions (for example, web servers, application servers, and database servers).

In the case that a specific configuration item is being considered, the population might be appropriately divided, and separate sample groups identified. For example, a sample of all servers may not be appropriate when reviewing an operating system configuration setting, where different operating systems are present within the environment. In this case, samples from each operating system type would be appropriate in identifying that the configuration has been appropriately set for each operating system. Each sample set should include servers that are representative of each operating system type, including version, as well as representative functions.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Other examples of sampling include selections of personnel with similar or varied roles, based on the requirement being assessed, for example, a sample of administrators vs. a sample of all employees.

The assessor is required to use professional judgment in the planning, performance, and evaluation of the sample to support their conclusion about whether and how the entity has met a requirement. The assessor's goal in sampling is to obtain enough evidence to have a reasonable basis for their opinion. When independently selecting samples, assessors should consider the following:

- The assessor must select the sample from the complete population without influence from the assessed entity.
- If the entity has standardized processes and controls in place that ensure consistency and which is applied to each item in the population, the sample can be smaller than if the entity has no standardized processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that items in the population adhere to the standardized processes that are applied to each item in the population. The assessor must verify that the standardized controls are implemented and working effectively.
- If the entity has more than one type of standardized process in place (for example, for different types of business facilities/system components), the sample must include items subject to each type of process. For example, populations could be divided into sub-populations based on characteristics that may impact the consistency of the assessed requirements, such as the use of different processes or tools. Samples would then be selected from each sub-population.
- If the entity has no standardized PCI DSS processes/controls in place and each item in the population is managed through non-standardized processes, the sample must be larger for the assessor to be assured that the PCI DSS requirements are appropriately applied to each item in the population.
- Samples of system components must include every type and combination being used. When an entity has more than one CDE, samples must include populations across all in-scope system components. For example, where applications are sampled, the sample must include all versions and platforms for each type of application.
- Sample sizes must always be greater than one unless there is only one item in the given population, or an automated control is used where the assessor has confirmed the control is functioning as programmed for each assessed sample population.
- If the assessor relies on standardized processes and controls being in place as a basis for selecting a sample, but then finds out during testing that standardized processes and controls are not in place or not operating effectively, the assessor should then increase the sample size to attempt to gain assurance that PCI DSS requirements are being met.

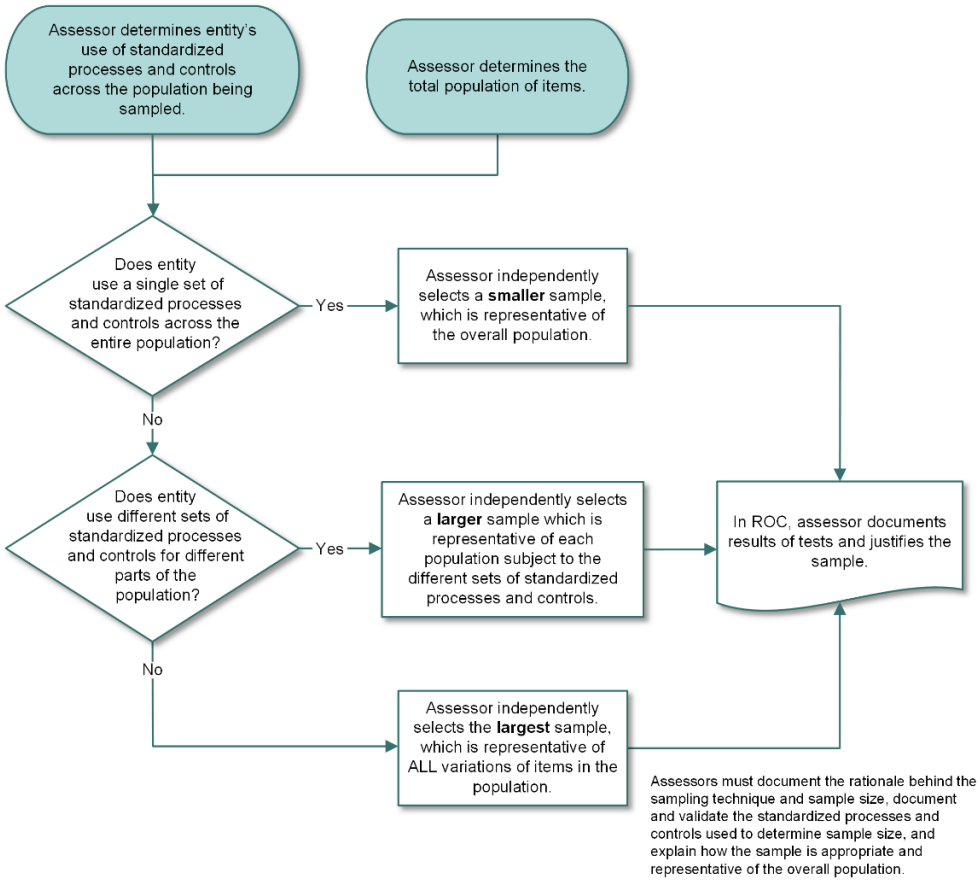
For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size.
- Validate and document the standardized processes and controls used to determine sample size.
- Explain how the sample is appropriate and representative of the overall population.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Figure 3 shows considerations for determining sample size.

Figure 3. PCI DSS Sampling Considerations



***Note**: In PCI DSS v4.0, specific references to sampling have been removed from all testing procedures. These references were removed because calling out sampling only in some testing procedures may have implied that sampling was mandatory for those testing procedures (which it was not) or that sampling was only allowable where it was specifically mentioned. Assessors should select samples when it is appropriate to the population being tested, and, per above, render those decisions after considering the overall scope and complexity of an environment.*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

7 Description of Timeframes Used in PCI DSS Requirements

Certain PCI DSS requirements have been established with specific timeframes for activities that need to be performed consistently via a regularly scheduled and repeatable process. The intent is that the activity is performed at an interval as close to that timeframe as possible without exceeding it. The entity has the discretion to perform an activity more often than specified (for example, performing an activity monthly where the PCI DSS requirement specifies it be performed every three months).

Table 4 outlines the frequency for the different time periods used in PCI DSS Requirements.

Table 4. PCI DSS Requirement Timeframes

Timeframes in PCI DSS Requirements	Descriptions and Examples
Daily	Every day of the year (not only on business days).
Weekly	At least once every seven days.
Monthly	At least once every 30 to 31 days, or on the nth day of the month.
Every three months ("quarterly")	At least once every 90 to 92 days, or on the nth day of each third month.
Every six months	At least once every 180 to 184 days, or on the nth day of each sixth month.
Every 12 months ("annually")	At least once every 365 (or 366 for leap years) days or on the same date every year.
Periodically	Frequency of occurrence is at the entity's discretion and is documented and supported by the entity's risk analysis. The entity must demonstrate that the frequency is appropriate for the activity to be effective and to meet the intent of the requirement.
Immediately	Without delay. In real time or near real time.
Promptly	As soon as reasonably possible.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Timeframes in PCI DSS Requirements	Descriptions and Examples
Significant change	There are several requirements that specify activities to be performed upon a significant change in an entity's environment. While what constitutes a significant change is highly dependent on the configuration of a given environment, each of the following activities, at a minimum, has potential impacts on the security of the CDE and must be considered and evaluated to determine whether a change is a significant change for an entity in the context of related PCI DSS requirements: • New hardware, software, or networking equipment added to the CDE. • Any replacement or major upgrades of hardware and/or software in the CDE. • Any changes in the flow or storage of account data. • Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment. • Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging, and monitoring). • Any changes to third-party vendors/service providers (or services provided) that support the CDE or meet PCI DSS requirements on behalf of the entity.

For other PCI DSS requirements, where the standard does not define a minimum frequency for recurring activities but instead allows for the requirement to be met "periodically," the entity is expected to define the frequency as appropriate for its business. The frequency defined by the entity must be supported by the entity's security policy and the risk analysis conducted according to PCI DSS Requirement 12.3.1. The entity must also be able to demonstrate that the frequency it has defined is appropriate for the activity to be effective and to meet the intent of the requirement.

In both cases, where PCI DSS specifies a required frequency and where PCI DSS allows for "periodic" performance, the entity is expected to have documented and implemented processes to ensure that activities are performed within a reasonable timeframe, including at least the following:

- The entity is promptly notified any time an activity is not performed per its defined schedule,
- The entity determines the events that led to missing a scheduled activity,
- The entity performs the activity as soon as possible after it is missed and either gets back on schedule or establishes a new schedule,
- The entity produces documentation that shows the above elements occurred.

When an entity has the above processes in place to detect and address when a scheduled activity is missed, a reasonable approach is allowable, meaning that if an activity is required to be performed at least once every three months, the entity is not automatically non-compliant if the activity is performed late where the entity's documented and implemented process (per above) was followed. However, where no such process is in place and/or the activity was not performed according to schedule due to oversight, mismanagement, or lack of

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

monitoring, the entity has not met the requirement. In such cases, the requirement will only be in place when the entity 1) documents (or reconfirms) the process per above to ensure the scheduled activity occurs on time, 2) re-establishes the schedule, and 3) provides evidence that the entity has performed the scheduled activity at least once per their schedule.

***Note**: Where an entity is being assessed for the first time against a PCI DSS requirement with a defined timeframe, it is considered an initial PCI DSS assessment for that requirement. This means the entity has never undergone a prior assessment to that requirement, where the assessment resulted in submission of a compliance validation document (for example, an AOC, SAQ, or ROC).*

For an initial assessment against a requirement that has a defined timeframe, it is not required that the activity has been performed for every such timeframe during the previous year, if the assessor verifies:

- *The activity was performed in accordance with the applicable requirement within the most recent timeframe (for example, the most recent three-month or six-month period), and*
- *The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.*

For subsequent years after the initial assessment, the activity must have been performed at least once within each required timeframe. For example, an activity required at least every three months must have been performed at least four times during the previous year at an interval that does not exceed 90-92 days.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

8 Approaches for Implementing and Validating PCI DSS

To support flexibility in how security objectives are met, there are two approaches for implementing and validating to PCI DSS. Entities should identify the approach best suited to their security implementation and use that approach to validate the controls.

Defined Approach	Follows the traditional method for implementing and validating PCI DSS and uses the Requirements and Testing Procedures defined within the standard. In the defined approach, the entity implements security controls to meet the stated requirements, and the assessor follows the defined testing procedures to verify that requirements have been met. The defined approach supports entities with controls in place that meet PCI DSS requirements as stated. This approach may also suit entities that want more direction about how to meet security objectives, as well as entities new to information security or PCI DSS. **Compensating Controls** As part of the defined approach, entities that cannot meet a PCI DSS requirement explicitly as stated due to a legitimate and documented technical or business constraint may implement other, or *compensating, controls*, that sufficiently mitigate the risk associated with not meeting the requirement. On an annual basis, any compensating controls must be documented by the entity and reviewed and validated by the assessor and included with the Report on Compliance submission. ***Note:*** *For more details, see Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.*
Customized Approach	Focuses on the Objective of each PCI DSS requirement (if applicable), allowing entities to implement controls to meet the requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. Because each customized implementation will be different, there are no defined testing procedures; the assessor is required to derive testing procedures that are appropriate to the specific implementation to validate that the implemented controls meet the stated Objective. ***Note:*** *For more details, see Appendix D: Customized Approach and PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website. The customized approach supports innovation in security practices, allowing entities greater flexibility to show how their current security controls meet PCI DSS objectives. This approach is intended for risk-mature entities that demonstrate a robust risk-management approach to security, including, but not limited to, a dedicated risk-management department or an organization-wide risk management approach. The controls implemented and validated using the customized approach are expected to meet or exceed the security provided by the requirement in the defined approach. The level of documentation and effort required to validate customized implementations will also be greater than for the defined approach

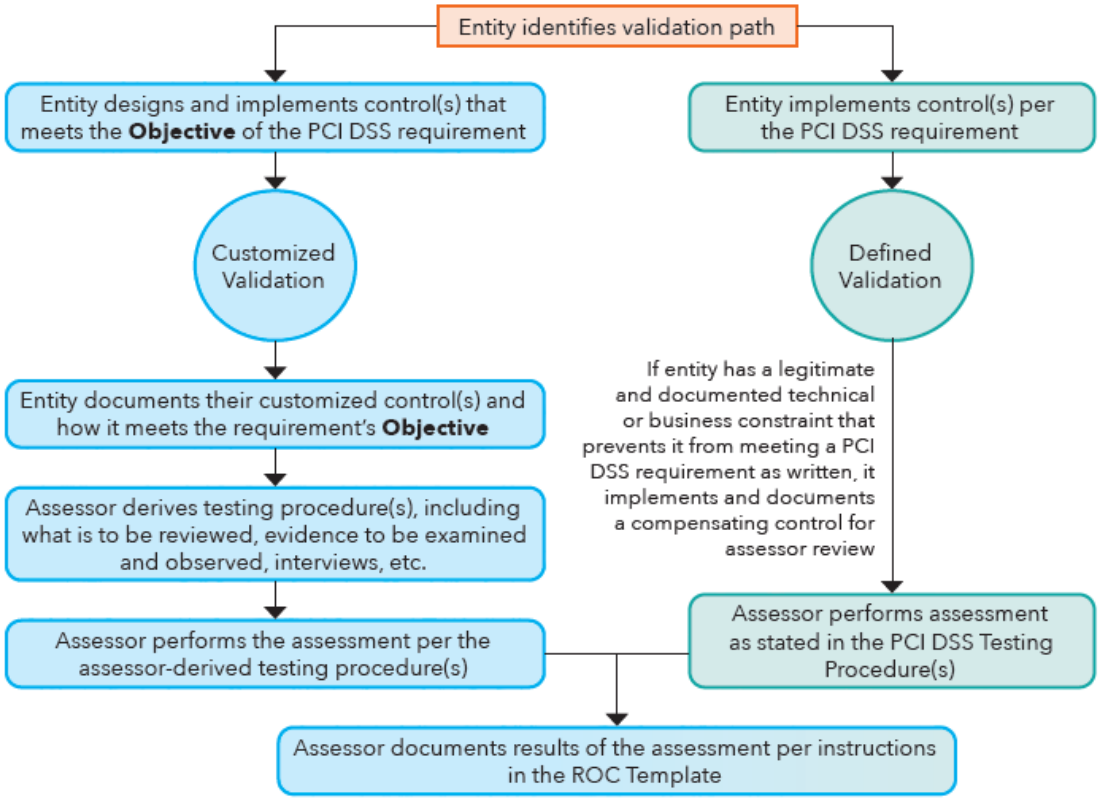
©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Most PCI DSS requirements can be met using either the defined or customized approach. However, several requirements do not have a stated Customized Approach Objective; the customized approach is not an option for these requirements.

Entities can use both the defined and customized approaches within their environment. This means an entity could use the defined approach to meet some requirements and use the customized approach to meet other requirements. This also means that an entity could use the defined approach to meet a given PCI DSS requirement for one system component or within one environment and use the customized approach to meet that same PCI DSS requirement for a different system component or within a different environment. In this way, a PCI DSS assessment could include both defined and customized testing procedures.

Figure 4 shows the two validation options for PCI DSS v4.x.

Figure 4. PCI DSS Validation Approaches



©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

9 Protecting Information About an Entity's Security Posture

The processes related to becoming and maintaining a PCI DSS compliant environment results in many artifacts that an entity may consider sensitive and may want to protect as such, including such items as the following:

- The Report on Compliance or Self-Assessment Questionnaire (the associated Attestation of Compliance is not considered sensitive and third-party service providers (TPSPs) are expected to share their AOC with customers).
- Network diagrams and account data-flow diagrams, and security configurations and rules.
- System configuration standards.
- Cryptography and key management methods and protocols.

Entities should review all the artifacts related to PCI DSS controls or the assessment and protect them in accordance with the entity's security policies for this type of information.

TPSPs are required (PCI DSS Requirement 12.9) to support their customers with the following:

- Information needed for customers to monitor the TPSPs' PCI DSS compliance status (to enable the customer to comply with Requirement 12.8), and
- Evidence that the TPSP is meeting applicable PCI DSS requirements where the TPSP's services are intended to meet or facilitate meeting a customer's PCI DSS requirements, or where those services may impact the security of a customer's cardholder data and/or sensitive authentication data.

This section does not impact or negate a TPSP's obligation to support and provide information to their customers per Requirement 12.9.

For more details about expectations for TPSPs and relationships between TPSPs and customers, see *Use of Third-Party Service Providers*.

Protection of Confidential and Sensitive Information by Qualified Security Assessor Companies

Each Qualified Security Assessor (QSA) Company signs an agreement with PCI SSC that they will adhere to the Qualification Requirements for QSAs. The *Protection of Confidential and Sensitive Information* section of that document includes the following:

> "The QSA company must have and adhere to a documented process for protection of confidential and sensitive information. This must include adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.
>
> "The QSA Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties and obligations as a QSA Company, unless (and to the extent) disclosure is required by legal authority."

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

10 Testing Methods for PCI DSS Requirements

The testing methods identified in the Testing Procedures for each requirement describe the expected activities to be performed by the assessor to determine whether the entity has met the requirement. The intent behind each testing method is described as follows:

- Examine: The assessor critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The assessor watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.
- Interview: The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The testing methods are intended to allow the assessed entity to demonstrate how they have met a requirement. They also provide the assessed entity and the assessor with a common understanding of the assessment activities to be performed. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and each entity's particular implementation. When documenting the assessment results, the assessor identifies the testing activities performed and the result of each activity.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

11 Instructions and Content for Report on Compliance

Instructions and content for the Report on Compliance (ROC) are provided in the *PCI DSS Report on Compliance (ROC) Template*.

The PCI DSS Report on Compliance (ROC) Template must be used as the template for creating a PCI DSS Report on Compliance.

Whether any entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (such as payment brands and acquirers). Entities should contact these organizations to determine any reporting requirements and instructions.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

12 PCI DSS Assessment Process

The PCI DSS assessment process includes the following high-level steps: [5]

1. Confirm the scope of the PCI DSS assessment.
2. Perform the PCI DSS assessment of the environment.
3. Complete the applicable report for the assessment according to PCI DSS guidance and instructions.
4. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Official Attestations of Compliance are only available on the PCI SSC website.
5. Submit the applicable PCI SSC documentation and the Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those that manage compliance programs such as payment brands and acquirers (for merchants), or other requesters (for service providers)).
6. If required, perform remediation to address requirements that are not in place and provide an updated report.

Note: *PCI DSS requirements are not considered to be in place if controls are not yet implemented or are scheduled to be completed at a future date. After any open or not-in-place items are addressed by the entity, the assessor will reassess to validate that the remediation is completed and that all requirements are satisfied. Refer to the following resources (available on the PCI SSC website) to document the PCI DSS assessment:*

- *For instructions about completing reports on compliance (ROC), refer to the PCI DSS Report on Compliance (ROC) Template.*
- *For instructions about completing self-assessment questionnaires (SAQ), refer to the PCI DSS SAQ Instructions and Guidelines.*
- *For instructions about submitting PCI DSS compliance validation reports, refer to the PCI DSS Attestation of Compliance.*

[5] The PCI DSS assessment process, and the roles and responsibilities for completion of each step, vary depending on the type of assessment and on compliance programs, which are managed by payment brands and acquirers.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

13 Additional References

Table 5 lists external organizations referenced within PCI DSS requirements or related guidance. These external organizations and their references are provided as information only and do not replace or extend any PCI DSS requirement.

Table 5. External Organizations Referenced in PCI DSS Requirements

Reference	Full Name
ANSI	American National Standards Institute
CIS	Center for Internet Security
CSA	Cloud Security Alliance
ENISA	European Union Agency for Cybersecurity (formerly European Network and Information Security Agency)
FIDO Alliance	The FIDO Alliance
ISO	International Organization for Standardization
NCSC	The UK National Cyber Security Centre
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
SAFECode	Software Assurance Forum for Excellence in Code

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

14 PCI DSS Versions

As of the published date of this document, PCI DSS v4.0.1 is the current version of the standard.

Questions about the use of previous versions should be directed to those organizations that manage compliance programs (such as payment brands and acquirers).

Table 6 summarizes PCI DSS versions and their relevant dates. [6]

Table 6. PCI DSS Versions

Version	Published	Retired
PCI DSS v4.0.1 (this document)	June 2024	To be determined
PCI DSS v4.0	March 2022	31 December 2024
PCI DSS v3.2.1	May 2018	31 March 2024
PCI DSS 3.2	April 2016	31 December 2018

[6] Subject to change upon release of a new version of PCI DSS.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

15 Detailed PCI DSS Requirements and Testing Procedures

Figure 5 describes the column headings and content for the PCI DSS requirements.

Figure 5. Understanding the Parts of the Requirements

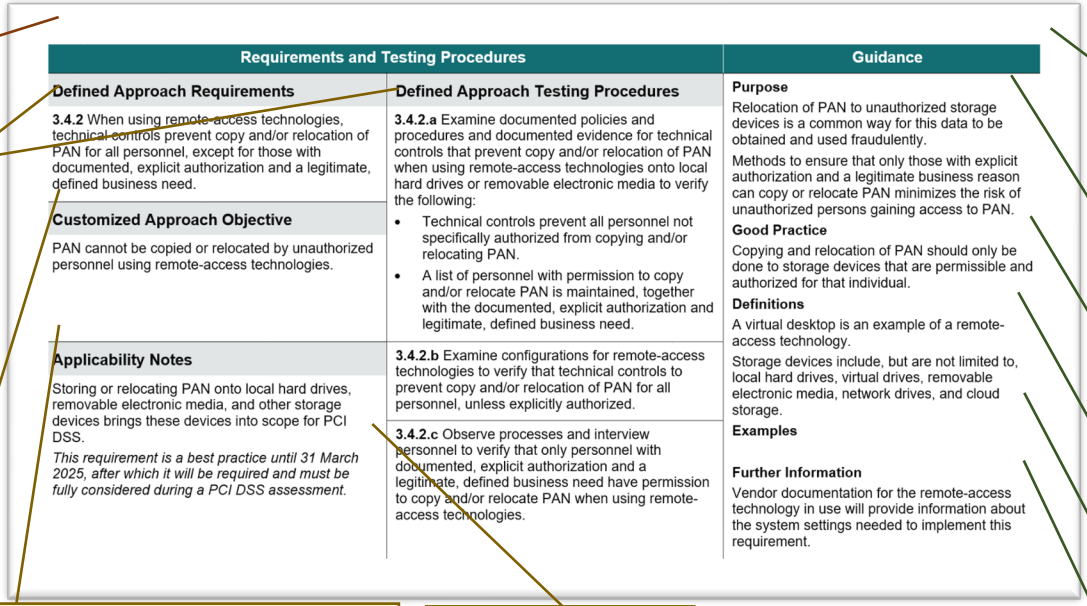
The **Requirement Description** at the X.X level organizes and describes the requirements that fall under it.

The **Defined Approach Requirements and Testing Procedures** describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

The **Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. **Definitions** A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. **Examples** **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized. **3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	

Applicability Notes apply to both the Defined and Customized Approach. It includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.x requirement with an extended implementation period.

Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.

Not every **Guidance** section described here is present for each requirement.

Not every section will be present for each requirement.

Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists.

A **Good Practice** can be considered by the entity when meeting a requirement.

Definitions Terms that may help understand the requirement.

Examples describe ways a requirement could be met.

Further Information includes references to relevant external documentation.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Additional Requirements for Service Providers Only

Some requirements apply only when the entity being assessed is a service provider. These are identified within the requirement as "*Additional requirement for service providers only"* and apply in addition to all other applicable requirements. Where the entity being assessed is both a merchant and a service provider, requirements noted as "*Additional requirement for service providers only"* apply to the service provider portion of the entity's business. Requirements identified with "*Additional requirement for service providers only"* are also recommended as best practices for consideration by all entities.

Appendices with Additional PCI DSS Requirements for Different Types of Entities

In addition to the 12 principal requirements, PCI DSS Appendix A contains additional PCI DSS requirements for different types of entities. The sections within Appendix A include:

- Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers.
- Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.
- Appendix A3: Designated Entities Supplemental Validation (DESV).

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Sections	
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.
1.2	Network security controls (NSCs) are configured and maintained.
1.3	Network access to and from the cardholder data environment is restricted.
1.4	Network connections between trusted and untrusted networks are controlled.
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Overview

Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined *policies* or *rules*.

NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

NSCs are used to control traffic within an entity's own networks—for example, between highly sensitive and less sensitive areas—and also to protect the entity's resources from exposure to untrusted networks. The cardholder data environment (CDE) is an example of a more sensitive area within an entity's network. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into sensitive systems. NSCs provide a key protection mechanism for any computer network.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For these reasons, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**1.**1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="4">Purpose
If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur.
Good Practice
Roles and responsibilities may be documented within policies and procedures or maintained within separate documents.
As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities.
Examples
A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).</td></tr>
<tr><td rowspan="2">1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.</td><td>1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.</td></tr>
<tr><td rowspan="2">1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.</td></tr>
<tr><td>Customized Approach Objective</td></tr>
<tr><td colspan="2">Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.</td></tr>
</table>

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.2 Network security controls (NSCs) are configured and maintained.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset). **Good Practice** These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network. **Definitions** NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE. Configuration standards outline an entity's minimum requirements for the configuration of its NSCs. **Examples** Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	**1.2.1.a** Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.	
	1.2.1.b Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.	
Customized Approach Objective		
The way that NSCs are configured and operate are defined and consistently applied.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Following a structured change control process for all changes to NSCs reduces the risk that a change could introduce a security vulnerability. **Good Practice** Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected. To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented. Once approved and verified, network documentation should be updated to include the changes to prevent inconsistencies between network documentation and the actual configuration.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	**1.2.2.a** Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.	
	1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.	
Customized Approach Objective	**1.2.2.c** Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.	
Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.		
Applicability Notes		
Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE. **Good Practice** All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams: • All locations, including retail locations, data centers, corporate locations, cloud providers, etc. • Clear labeling of all network segments. • All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version). • All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc. *(continued on next page)*
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	**1.2.3.a** Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.	
Customized Approach Objective		
A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.	**1.2.3.b** Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.	
Applicability Notes		
A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.2.3 *(continued)*		• Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism. • Date of last update, and names of people that made and approved the updates. • A legend or key to explain the diagram. Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	**1.2.4.a** Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement.	An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices. Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured.
Customized Approach Objective	**1.2.4.b** Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.	**Good Practice**
A representation of all transmissions of account data between system components and across network segments is maintained and available.		The data-flow diagram should include all connection points where account data is received into and sent out of the network, including connections to open, public networks, application processing flows, storage, transmissions between systems and networks, and file backups.
Applicability Notes		*(continued on next page)*
A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.2.4 *(continued)*		The data-flow diagram is meant to be in addition to the network diagram and should reconcile with and augment the network diagram. As a best practice, entities can consider including the following in their data-flow diagrams: • All processing flows of account data, including authorization, capture, settlement, chargeback, and refunds. • All distinct acceptance channels, including card-present, card-not-present, and e-commerce. • All types of data receipt or transmission, including any involving hard copy/paper media. • The flow of account data from the point where it enters the environment, to its final disposition. • Where account data is transmitted and processed, where it is stored, and whether storage is short term or long term. • The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared. • Date of last update, and names of people that made and approved the updates.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed. **Good Practice** The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	**1.2.5.a** Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.	
	1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.	
Customized Approach Objective		
Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="4">Purpose
Compromises take advantage of insecure network configurations.
Good Practice
If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity.
Further Information
For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).</td></tr>
<tr><td rowspan="2">1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.</td><td>1.2.6.a Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.</td></tr>
<tr><td>1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.</td></tr>
<tr><td>Customized Approach Objective</td><td></td></tr>
<tr><td>The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.</td><td></td><td></td></tr>
</table>

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Such a review gives the organization an opportunity to clean up any unneeded, outdated, or incorrect rules and configurations which could be utilized by an unauthorized person. Furthermore, it ensures that all rules and configurations allow only authorized services, protocols, and ports that match the documented business justifications. **Good Practice** This review, which can be implemented using manual, automated, or system-based methods, is intended to confirm that the settings that manage traffic rules, what is allowed in and out of the network, match the approved configurations. The review should provide confirmation that all permitted access has a justified business reason. Any discrepancies or uncertainties about a rule or configuration should be escalated for resolution. While this requirement specifies that this review occur at least once every six months, organizations with a high volume of changes to their network configurations may wish to consider performing reviews more frequently to ensure that the configurations continue to meet the needs of the business.
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	**1.2.7.a** Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.	
	1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.	
Customized Approach Objective	**1.2.7.c** Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.	
NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** To prevent unauthorized configurations from being applied to the network, stored files with configurations for network controls need to be kept up to date and secured against unauthorized changes. Keeping configuration information current and secure ensures that the correct settings for NSCs are applied whenever the configuration is run. **Examples** If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	**1.2.8** Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.	
Customized Approach Objective		
NSCs cannot be defined or modified using untrusted configuration objects (including files).		
Applicability Notes		
Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.3 Network access to and from the cardholder data environment is restricted.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner. **Good Practice** All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content. **Examples** Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**1.3.1.a** Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.	
Customized Approach Objective	**1.3.1.b** Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.	
Unauthorized traffic cannot enter the CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host. **Good Practice** All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content. **Examples** Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**1.3.2.a** Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.	
Customized Approach Objective	**1.3.2.b** Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.	
Unauthorized traffic cannot leave the CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	**1.3.3** Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.4 Network connections between trusted and untrusted networks are controlled.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Implementing NSCs at every connection coming into and out of trusted networks allows the entity to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection. **Examples** An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.
1.4.1 NSCs are implemented between trusted and untrusted networks.	**1.4.1.a** Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.	
	1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.	
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Ensuring that public access to a system component is specifically authorized reduces the risk of system components being unnecessarily exposed to untrusted networks. **Good Practice** System components that provide publicly accessible services, such as email, web, and DNS servers, are the most vulnerable to threats originating from untrusted networks. Ideally, such systems are placed within a dedicated trusted network that is public facing (for example, a DMZ) but that is separated via NSCs from more sensitive internal systems, which helps protect the rest of the network in the event these externally accessible systems are compromised. This functionality is intended to prevent malicious actors from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner. Where this functionality is provided as a built-in feature of an NSC, the entity should ensure that its configurations do not result in the functionality being disabled or bypassed. **Definitions** Maintaining the "state" (or status) for each connection into a network means the NSC "knows" whether an apparent response to a previous connection is a valid, authorized response (since the NSC retains each connection's status) or whether it is malicious traffic trying to fool the NSC into allowing the connection.
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	**1.4.2** Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.		
Applicability Notes		
The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Filtering packets coming into the trusted network helps to, among other things, ensure packets are not “spoofed” to appear as if they are coming from an organization’s own internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ. **Good Practice** Products usually come with anti-spoofing set as a default and may not be configurable. Entities should consult the vendor's documentation for more information. **Examples** Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Malicious individuals will often try to spoof (or imitate) the sending IP address to fool the target system into believing the packet is from a trusted source.
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. **Customized Approach Objective** Packets with forged IP source addresses cannot enter a trusted network.	**1.4.3** Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	**1.4.4.a** Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.	Cardholder data that is directly accessible from an untrusted network, for example, because it is stored on a system within the DMZ or in a cloud database service, is easier for an external attacker to access because there are fewer defensive layers to penetrate. Using NSCs to ensure that system components that store cardholder data (such as a database or a file) can only be directly accessed from trusted networks can prevent unauthorized network traffic from reaching the system component.
Customized Approach Objective	**1.4.4.b** Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.	
Stored cardholder data cannot be accessed from untrusted networks.		
Applicability Notes		
This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting the disclosure of internal, private, and local IP addresses is useful to prevent a hacker from obtaining knowledge of these IP addresses and using that information to access the network. **Good Practice** Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks. **Examples** Methods to obscure IP addressing may include, but are not limited to: • IPv4 Network Address Translation (NAT). • Placing system components behind proxy servers/NSCs. • Removal or filtering of route advertisements for internal networks that use registered addressing. • Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	**1.4.5.a** Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.	
	1.4.5.b Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.	
Customized Approach Objective		
Internal network information is protected from unauthorized disclosure.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	**1.5.1.a** Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement. **1.5.1.b** Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.	Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats. Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, network-based heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network. *(continued on next page)*
Customized Approach Objective		
Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.		**Good Practice** The specific configuration settings are determined by the entity and should be consistent with its network security policies and procedures. Where there is a legitimate need to temporarily disable security controls on a company-owned or employee-owned device that connects to both an untrusted network and the CDE—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action is understood and approved by an appropriate management representative. Any disabling or altering of these security controls, including on administrators' own devices, is performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable security controls on their own computers, but there should be alerting mechanisms in place when such controls are disabled and follow up that occurs to ensure processes were followed. **Examples** Practices include forbidding split-tunneling of VPNs for employee-owned or corporate-owned mobile devices and requiring that such devices boot up into a VPN.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 2: Apply Secure Configurations to All System Components

Sections
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.
2.2 System components are configured and managed securely.
2.3 Wireless environments are configured and managed securely.

Overview

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**2.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	**2.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned.	
	2.1.2.b Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
2.2 System components are configured and managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	**2.2.1.a** Examine system configuration standards to verify they define processes that include all elements specified in this requirement. **2.2.1.b** Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. **2.2.1.c** Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.	**Purpose** There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity's environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker. By developing standards, entities ensure their system components will be configured consistently and securely and will address the protection of devices for which full hardening may be more difficult. **Good Practice** Keeping up to date with current industry guidance will help the entity maintain secure configurations. The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system. Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses. **Further Information** Sources for guidance on configuration standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, and product vendors.
Customized Approach Objective		
All system components are configured securely and consistently and in accordance with industry-accepted hardening standards or vendor recommendations.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals often use vendor default account names and passwords to compromise operating systems, applications, and the systems on which they are installed. Because these default settings are often published and are well known, changing these settings will make systems less vulnerable to attack. **Good Practice** All vendor default accounts should be identified, and their purpose and use understood. It is important to establish controls for application and system accounts, including those used to deploy and maintain cloud services so that they do not use default passwords and are not usable by unauthorized individuals. Where a default account is not intended to be used, changing the default password to a unique password that meets PCI DSS Requirement 8.3.6, removing any access to the default account, and then disabling the account, will prevent a malicious individual from re-enabling the account and gaining access with the default password. Using an isolated staging network to install and configure new systems is recommended and can also be used to confirm that default credentials have not been introduced into production environments. **Examples** Defaults to be considered include user IDs, passwords, and other authentication credentials commonly used by vendors in their products.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	**2.2.2.a** Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.	
	2.2.2.b Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective System components cannot be accessed using default passwords.	**2.2.2.c** Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.	
Applicability Notes This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Systems containing a combination of services, protocols, and daemons for their primary function will have a security profile appropriate to allow that function to operate effectively. For example, systems that need to be directly connected to the Internet would have a particular profile, like a DNS server, web server, or an e-commerce server. Conversely, other system components may operate a primary function comprising a different set of services, protocols, and daemons that perform functions that an entity does not want exposed to the Internet. This requirement aims to ensure that different functions do not impact the security profiles of other services in a way which may cause them to operate at a higher or lower security level. **Good Practice** Ideally, each function should be placed on different system components. This can be achieved by implementing only one primary function on each system component. Another option is to isolate primary functions on the same system component that have different security levels, for example, isolating web servers (which need to be directly connected to the Internet) from application and database servers. *(continued on next page)*
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from each other, **OR** • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	**2.2.3.a** Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement. **2.2.3.b** Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement. **2.2.3.c** Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the following ways: • Functions with differing security needs do not co-exist on the same system component. • Functions with differing security needs that exist on the same system component are isolated from each other. • Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.	
Customized Approach Objective		
Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
2.2.3 *(continued)*		If a system component contains primary functions that need different security levels, a third option is to implement additional controls to ensure that the resultant security level of the primary function(s) with higher security needs is not reduced by the presence of the lower security primary functions. Additionally, the functions with a lower security level should be isolated and/or secured to ensure they cannot access or affect the resources of another system function, and do not introduce security weaknesses to other functions on the same server. Functions of differing security levels may be isolated by either physical or logical controls. For example, a database system should not also be hosting web services unless using controls like virtualization technologies to isolate and contain the functions into separate sub-systems. Another example is using virtual instances or providing dedicated memory access by system function. Where virtualization technologies are used, the security levels should be identified and managed for each virtual component. Examples of considerations for virtualized environments include: • The function of each application, container, or virtual server instance. • How virtual machines (VMs) or containers are stored and secured.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Unnecessary services and functions can provide additional opportunities for malicious individuals to gain access to a system. By removing or disabling all unnecessary services, protocols, daemons, and functions, organizations can focus on securing the functions that are required and reduce the risk that unknown or unnecessary functions will be exploited. **Good Practice** There are many protocols that could be enabled by default that are commonly used by malicious individuals to compromise a network. Disabling or removing all services, functions, and protocols that are not used minimizes the potential attack surface—for example, by removing or disabling an unused FTP or web server. **Examples** Unnecessary functionality may include, but is not limited to scripts, drivers, features, subsystems, file systems, interfaces (USB and Bluetooth), and unnecessary web servers.
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	**2.2.4.a** Examine system configuration standards to verify necessary services, protocols, daemons, and functions are identified and documented.	
	2.2.4.b Examine system configurations to verify the following: • All unnecessary functionality is removed or disabled. • Only required functionality, as documented in the configuration standards, is enabled.	
Customized Approach Objective		
System components cannot be compromised by exploiting unnecessary functionality present in the system component.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to exploit common points of compromise within a network. **Good Practice** Enabling security features before new system components are deployed will prevent insecure configurations from being introduced into the environment. Some vendor solutions may provide additional security functions to assist with securing an insecure process. **Further Information** For guidance on services, protocols, or daemons considered to be insecure, refer to industry standards and guidance (for example, as published by NIST, ENISA, and OWASP).
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	**2.2.5.a** If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.	
	2.2.5.b If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.	
Customized Approach Objective		
System components cannot be compromised by exploiting insecure services, protocols, or daemons.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Correctly configuring security parameters provided in system components takes advantage of the capabilities of the system component to defeat malicious attacks. **Good Practice** System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. For systems to be configured securely, personnel responsible for configuration and/or administering systems should be knowledgeable in the specific security parameters and settings that apply to the system. Considerations should also include secure settings for parameters used to access cloud portals. **Further Information** Refer to vendor documentation and industry references noted in Requirement 2.2.1 for information about applicable security parameters for each type of system.
2.2.6 System security parameters are configured to prevent misuse.	**2.2.6.a** Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.	
	2.2.6.b Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.	
Customized Approach Objective	**2.2.6.c** Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.	
System components cannot be compromised because of incorrect security parameter configuration.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If non-console (including remote) administration does not use encrypted communications, administrative authorization factors (such as IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. **Good Practice** Whichever security protocol is used, it should be configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates, supporting only strong encryption, and not supporting fallback to weaker, insecure protocols or methods. **Examples** Cleartext protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. Non-console access may be facilitated by technologies that provide alternative access to systems, including but not limited to, out-of-band (OOB), lights-out management (LOM), Intelligent Platform Management Interface (IPMI), and keyboard, video, mouse (KVM) switches with remote capabilities. These and other non-console access technologies and methods must be secured with strong cryptography. **Further Information** Refer to industry standards and best practices such as *NIST SP 800-52 and SP 800-57*.
2.2.7 All non-console administrative access is encrypted using strong cryptography.	**2.2.7.a** Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.	
	2.2.7.b Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.	
	2.2.7.c Examine settings for system components and authentication services to verify that insecure remote login services are not available for non-console administrative access.	
	2.2.7.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.	
Customized Approach Objective		
Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.		
Applicability Notes		
This includes administrative access via browser-based interfaces and application programming interfaces (APIs).		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
2.3 Wireless environments are configured and managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. **Good Practice** Wireless passwords should be constructed so that they are resistant to offline brute force attacks.
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	**2.3.1.a** Examine policies and procedures and interview responsible personnel to verify that processes are defined for wireless vendor defaults to either change them upon installation or to confirm them to be secure in accordance with all elements of this requirement.	
	2.3.1.b Examine vendor documentation and observe a system administrator logging into wireless devices to verify: • SNMP defaults are not used. • Default passwords/passphrases on wireless access points are not used.	
Customized Approach Objective	**2.3.1.c** Examine vendor documentation and wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.	
Wireless networks cannot be accessed using vendor default passwords or default configurations.		
Applicability Notes		
This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know. Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise. **Good Practice** This goal can be accomplished in multiple ways, including periodic changes of keys, changing keys via a defined "joiners-movers-leavers" (JML) process, implementing additional technical controls, and not using fixed pre-shared keys. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan at Requirement 12.10.1.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	**2.3.2** Interview responsible personnel and examine key-management documentation to verify that wireless encryption keys are changed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Protect Account Data

Requirement 3: Protect Stored Account Data

Sections	
3.1	Processes and mechanisms for protecting stored account data are defined and understood.
3.2	Storage of account data is kept to a minimum.
3.3	Sensitive authentication data (SAD) is not stored after authorization.
3.4	Access to displays of full PAN and ability to copy PAN are restricted.
3.5	Primary account number (PAN) is secured wherever it is stored.
3.6	Cryptographic keys used to protect stored account data are secured.
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

Overview

Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of PAN is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

Refer to *Appendix G* for definitions of “strong cryptography” and other PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.1 Processes and mechanisms for protecting stored account data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 3.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 3. While it is important to define the specific policies or procedures called out in Requirement 3, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**3.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	**3.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned.	
	3.1.2.b Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.2 Storage of account data is kept to a minimum.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time. **Good Practice** When identifying locations of stored account data, consider all processes and personnel with access to the data, as data could have been moved and stored in different locations than originally defined. Storage locations that are often overlooked include backup and archive systems, removable data storage devices, paper-based media, and audio recordings. To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes. *(continued on next page)*
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	**3.2.1.a** Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.	
	3.2.1.b Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.	
	3.2.1.c Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.	
Customized Approach Objective		
Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. *The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.*		Methods of eliminating data when it exceeds the retention period include secure deletion to complete removal of the data or rendering it unrecoverable and unable to be reconstructed. Identifying and securely eliminating stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated, manual, or a combination of both. The deletion function in most operating systems is not "secure deletion" as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable. *Remember, if you don't need it, don't store it!* **Examples** An automated, programmatic procedure could be run to locate and remove data, or a manual review of data storage areas could be performed. Whichever method is used, it is a good idea to monitor the process to ensure it is completed successfully, and that the results are recorded and validated as being complete. Implementing secure deletion methods ensures that the data cannot be retrieved when it is no longer needed. **Further Information** See *NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.3 Sensitive authentication data (SAD) is not stored after authorization.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.3.1 SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	**3.3.1.a** If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not stored after authorization.	SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited.
Customized Approach Objective	**3.3.1.b** If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.	**Good Practice** It may be acceptable for an entity to store SAD in non-persistent memory for a short time after authorization is complete, if following conditions are met: • There is a legitimate business need to access SAD in memory after authorization is complete. • SAD is only ever stored in non-persistent memory (for example, RAM, volatile memory). • Controls are in place to ensure that memory maintains a non-persistent state. • SAD is removed as soon as the business purpose is complete. It is not permissible to store SAD in persistent memory.
This requirement is not eligible for the customized approach.		**Definitions** The authorization process completes when a merchant receives a transaction response (for example, an approval or decline). Refer to *Appendix G* for the definition of “authorization.”
Applicability Notes		
Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer. Refer to Requirement 3.3.3 for additional requirements specifically for these entities. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.3.1.1 The full contents of any track are not stored upon completion of the authorization process.	**3.3.1.1** Examine data sources to verify that the full contents of any track are not stored upon completion of the authorization process.	If full contents of any track (from the magnetic stripe on the back of a card if present, equivalent data contained on a chip, or elsewhere) is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions. **Definitions** Full track data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Each track contains a number of data elements, and this requirement specifies only those that may be retained post-authorization. **Examples** Data sources to review to ensure that the full contents of any track are not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **3.3.1.2** The card verification code is not stored upon completion of the authorization process. **Customized Approach Objective** This requirement is not eligible for the customized approach. **Applicability Notes** The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.	**Defined Approach Testing Procedures** **3.3.1.2** Examine data sources, to verify that the card verification code is not stored upon completion of the authorization process.	**Purpose** If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised. **Examples** If card verification codes are stored on paper media prior to completion of authorization, a method of erasing or covering the codes should prevent them from being read after authorization is complete. Example methods of rendering the codes unreadable include removing the code with scissors and applying a suitably opaque and un-removable marker over the code. Data sources to review to ensure that the card verification code is not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.3.1.3 The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.	**3.3.1.3** Examine data sources, to verify that PINs and PIN blocks are not stored upon completion of the authorization process.	PIN and PIN blocks should be known only to the card owner or entity that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based transactions (for example, in-store purchases and ATM withdrawals). Not storing this data reduces the probability of it being compromised. **Examples** Data sources to review to ensure that PIN and PIN blocks are not retained upon completion of the authorization process include, but are not limited to: • Incoming transaction data. • All logs (for example, transaction, history, debugging, error). • History files. • Trace files. • Database schemas. • Contents of databases, and on-premise and cloud data stores. • Any existing memory/crash dump files.
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	**3.3.2** Examine data stores, system configurations, and/or vendor documentation to verify that all SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions. **Good Practice** Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.
Customized Approach Objective		
This requirement is not eligible for the customized approach. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact these organizations for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer. Refer to Requirement 3.3.3 for requirements specifically for these entities. This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Definitions** The authorization process is completed when a merchant receives a transaction response (for example, an approval or decline) . Refer to *Appendix G* for the definition of “authorization.”

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** SAD can be used by malicious individuals to increase the probability of successfully generating counterfeit payment cards and creating fraudulent transactions. **Good Practice** Entities should consider encrypting SAD with a different cryptographic key than is used to encrypt PAN. Note that this does not mean that PAN present in SAD (as part of track data) would need to be separately encrypted.
3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*	**3.3.3.a** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine documented policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.	
Customized Approach Objective	**3.3.3.b** ***Additional testing procedure for issuers and companies that support issuing services and store sensitive authentication data:*** Examine data stores and system configurations to verify that the sensitive authentication data is stored securely.	
Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only to issuers and companies that support issuing services and store sensitive authentication data. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. A legitimate issuing business need is one that is necessary for the performance of the function being provided by or for the issuer. *The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.4 Access to displays of full PAN and ability to copy PAN are restricted.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
3.4.1 PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN. *(continued on next page)*	**3.4.1.a** Examine documented policies and procedures for masking the display of PANs to verify: • A list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN is masked when displayed such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs.	**Purpose** The display of full PAN on computer screens, payment card receipts, paper reports, etc. can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that the full PAN is displayed only for those with a legitimate business need minimizes the risk of unauthorized persons gaining access to PAN data. **Good Practice** Applying access controls according to defined roles is one way to limit access to viewing full PAN to only those individuals with a defined business need. The masking approach should always display only the number of digits needed to perform a specific business function. For example, if only the last four digits are needed to perform a business function, PAN should be masked to only show the last four digits. As another example, if a function needs to view the bank identification number (BIN) for routing purposes, unmask only the BIN digits for that function. *(continued on next page)*
	3.4.1.b Examine system configurations to verify that full PAN is only displayed for roles with a documented business need, and that PAN is masked for all other requests.	
	3.4.1.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displayed, and that only those with a legitimate business need are able to see more than the BIN and/or last four digits of the PAN.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective PAN displays are restricted to the minimum number of digits necessary to meet a defined business need. **Applicability Notes** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.		**Definitions** Masking is not synonymous with truncation and these terms cannot be used interchangeably. Masking refers to the concealment of certain digits during display or printing, even when the entire PAN is stored on a system. This is different from truncation, in which the truncated digits are removed and cannot be retrieved within the system. Masked PAN could be “unmasked”, but there is no "un-truncation" without recreating the PAN from another source. Refer to *Appendix G* for definitions of “masking” and “truncation.” **Further Information** For more information about masking and truncation, see PCI SSC’s FAQs on these topics.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. **Definitions** A virtual desktop is an example of a remote-access technology. Such remote access technologies often include tools to disable copy and/or relocation functionality. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	**3.4.2.a** Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**3.4.2.b** Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized. **3.4.2.c** Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.5 Primary account number (PAN) is secured wherever it is stored.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures.	**3.5.1.a** Examine documentation about the system used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.b** Examine data repositories and audit logs, including payment application logs, to verify the PAN is rendered unreadable using any of the methods specified in this requirement. **3.5.1.c** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	Rendering stored PAN unreadable is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. **Good Practice** It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed versions of a PAN. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable. Implementing keyed cryptographic hashes with associated key management processes and procedures in accordance with Requirement 3.5.1.1 is a valid additional control to prevent correlation. **Further Information** For information about truncation formats and truncation in general, see PCI SSC's FAQs on the topic. Sources for information about index tokens include: • PCI SSC's Tokenization Product Security Guidelines (*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*) • *ANSI X9.119-2-2017: Retail Financial Services - Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*
Customized Approach Objective		
Cleartext PAN cannot be read from storage media.		
Applicability Notes		
This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs). This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	**3.5.1.1.a** Examine documentation about the hashing method used to render PAN unreadable, including the vendor, type of system/process, and the encryption algorithms (as applicable) to verify that the hashing method results in keyed cryptographic hashes of the entire PAN, with associated key management processes and procedures.	Rendering stored PAN unreadable is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control. A hashing function that incorporates a randomly generated secret key provides brute force attack resistance and secret authentication integrity.
Customized Approach Objective	**3.5.1.1.b** Examine documentation about the key management procedures and processes associated with the keyed cryptographic hashes to verify keys are managed in accordance with Requirements 3.6 and 3.7.	**Definitions** Refer to *Appendix G* for the definition of "keyed cryptographic hash" and for information about appropriate keyed cryptographic hashing algorithms and additional resources.
Cleartext PAN cannot be determined from hashes of the PAN.	**3.5.1.1.c** Examine data repositories to verify the PAN is rendered unreadable.	**Examples** Systems which only have access to one hash value at a time and which store no other account data on the same system as the hash, are not required to meet key-management processes and procedures (Requirements 3.6 and 3.7). Examples of such systems include transaction-originating devices that generate a hash of the PAN for use in a backend system, such as pay-at-gate transit turnstiles. However, in such an implementation, the backend system will have access to more than one hash value at a time, and therefore is required to meet key-management processes and procedures at Requirements 3.6 and 3.7.
Applicability Notes	**3.5.1.1.d** Examine audit logs, including payment application logs, to verify the PAN is rendered unreadable.	
All Applicability Notes for Requirement 3.5.1 also apply to this requirement.		
(continued on next page)		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
(continued) Key-management processes and procedures (Requirements 3.6 and 3.7) do not apply to system components used to generate individual keyed hashes of a PAN for comparison to another system if: • The system components only have access to one hash value at a time (hash values are not stored on the system) **AND** • There is no other account data stored on the same system as the hashes. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment. This requirement will replace the bullet in Requirement 3.5.1 for one-way hashes once its effective date is reached.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	**3.5.1.2.a** Examine encryption processes to verify that, if disk-level or partition-level encryption is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media, **OR** • If used for non-removable electronic media, examine encryption processes used to verify that PAN is also rendered unreadable via another method that meets Requirement 3.5.1.	Disk-level and partition-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. For this reason, disk-level encryption is not appropriate to protect stored PAN on computers, laptops, servers, storage arrays, or any other system that provides transparent decryption upon user authentication. **Further Information** Where available, following vendors' hardening and industry best practice guidelines can assist in securing PAN on these devices.
Customized Approach Objective	**3.5.1.2.b** Examine configurations and/or vendor documentation and observe encryption processes to verify the system is configured according to vendor documentation the result is that the disk or the partition is rendered unreadable.	
Encrypted PAN is only decrypted when there is a legitimate business need to access that PAN. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
(continued) This requirement applies to any encryption method that provides clear-text PAN automatically when a system runs, even though an authorized user has not specifically requested that data. While disk or partition encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices. Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies. Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. For issuers and companies that support issuing services: This requirement does not apply to PANs being accessed for real-time transaction processing. However, it does apply to PANs stored for other purposes. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	**3.5.1.3.a** If disk-level or partition-level encryption is used to render PAN unreadable, examine the system configuration and observe the authentication process to verify that logical access is implemented in accordance with all elements specified in this requirement.	**Purpose** Disk-level encryption typically encrypts the entire disk or partition using the same key, with all data automatically decrypted when the system runs or when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and perform the appropriate cryptographic transformations without any special action by the user other than supplying a password or passphrase at system start-up or at the beginning of a session. This provides no protection from a malicious individual that has already managed to gain access to a valid user account. **Good Practice** Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is best limited only to removable electronic media storage devices.
Customized Approach Objective	**3.5.1.3.b** Examine files containing authentication factors (passwords, passphrases, or cryptographic keys) and interview personnel to verify that authentication factors that allow access to unencrypted data are stored securely and are independent from the native operating system's authentication and access control methods.	
Disk encryption implementations are configured to require independent authentication and logical access controls for decryption.		
Applicability Notes		
Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.6 Cryptographic keys used to protect stored account data are secured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	**3.6.1** Examine documented key-management policies and procedures to verify that processes to protect cryptographic keys used to protect stored account data against disclosure and misuse are defined to include all elements specified in this requirement.	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. **Good Practice** Having a centralized key management system based on industry standards is recommended for managing cryptographic keys. **Further Information** The entity's key management procedures will benefit through alignment with industry requirements, Sources for information on cryptographic key management life cycles include: • *ISO 11568-1 Banking — Key management (retail) — Part 1*: Principles (specifically Chapter 10 and the referenced Parts 2 & 4) • *NIST SP 800-57 Part 1 Revision 5— Recommendation for Key Management, Part 1: General*.
Customized Approach Objective		
Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.		
Applicability Notes		
This requirement applies to keys used to protect stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect stored account data, as well as the devices that generate, use, and protect the keys. This allows an entity to keep pace with evolving threats to its architecture and plan for updates as the assurance level provided by different algorithms and key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices and identify unauthorized additions to its cryptographic architecture. The use of the same cryptographic keys in both production and test environments introduces a risk of exposing the key if the test environment is not at the same security level as the production environment. **Good Practice** Having an automated reporting mechanism can assist with maintenance of the cryptographic attributes.
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, to support meeting Requirement 12.3.4.	**3.6.1.1** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and examine documentation to verify that a document exists to describe the cryptographic architecture that includes all elements specified in this requirement.	
Customized Approach Objective		
Accurate details of the cryptographic architecture are maintained and available. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer. *The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
3.6.1.2 Secret and private keys used to protect stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	**3.6.1.2.a** Examine documented procedures to verify it is defined that cryptographic keys used to encrypt/decrypt stored account data must exist only in one (or more) of the forms specified in this requirement.	**Purpose** Storing cryptographic keys securely prevents unauthorized or unnecessary access that could result in the exposure of stored account data. Storing keys separately means they are stored such that if the location of one key is compromised, the second key is not also compromised. **Good Practice** Where data-encrypting keys are stored in an HSM, the HSM interaction channel should be protected to prevent interception of encryption or decryption operations.
	3.6.1.2.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt stored account data exist in one (or more) of the forms specified in this requirement.	
	3.6.1.2.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys.	
Customized Approach Objective		
Secret and private keys are stored in a secure form that prevents unauthorized retrieval or access. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		
Defined Approach Requirements **3.6.1.3** Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary. **Customized Approach Objective** Access to cleartext cryptographic key components is restricted to necessary personnel.	**Defined Approach Testing Procedures** **3.6.1.3** Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**Purpose** Restricting the number of people who have access to cleartext cryptographic key components reduces the risk of stored account data being retrieved or rendered visible by unauthorized parties. **Good Practice** Only personnel with defined key custodian responsibilities (creating, altering, rotating, distributing, or otherwise maintaining encryption keys) should be granted access to key components. Ideally this will be a very small number of people.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	**3.6.1.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	Storing any cryptographic keys in the fewest locations helps an organization track and monitor all key locations and minimizes the potential for keys to be exposed to unauthorized parties.
Customized Approach Objective		
Cryptographic keys are retained only where necessary.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of strong cryptographic keys significantly increases the level of security of encrypted account data. **Further Information** See the sources referenced at Cryptographic Key Generation in *Appendix G*.
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	**3.7.1.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define generation of strong cryptographic keys.	
	3.7.1.b Observe the method for generating keys to verify that strong keys are generated.	
Customized Approach Objective		
Strong cryptographic keys are generated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Secure distribution or conveyance of secret or private cryptographic keys means that keys are distributed only to authorized custodians, as identified in Requirement 3.6.1.2, and are never distributed insecurely.
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	**3.7.2.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure distribution of cryptographic keys.	
	3.7.2.b Observe the method for distributing keys to verify that keys are distributed securely.	
Customized Approach Objective		
Cryptographic keys are secured during distribution.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of account data. **Good Practice** Data encryption keys can be protected by encrypting them with a key-encrypting key. Keys can be stored in a Hardware Security Module (HSM). Secret or private keys that can decrypt data should never be present in source code.
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	**3.7.3.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define secure storage of cryptographic keys.	
	3.7.3.b Observe the method for storing keys to verify that keys are stored securely.	
Customized Approach Objective		
Cryptographic keys are secured when stored.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changing encryption keys when they reach the end of their cryptoperiod is imperative to minimize the risk of someone obtaining the encryption keys and using them to decrypt data. **Definitions** A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose. Cryptoperiods are often defined in terms of the period for which the key is active and/or the amount of cipher-text that has been produced by the key. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. **Further Information** *NIST SP 800-57 Part 1, Revision 5, Section 5.3 Cryptoperiods* – provides guidance for establishing the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect. See Table 1 of *SP 800-57* Part 1 for suggested cryptoperiods for different key types.
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	**3.7.4.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data to verify that they define changes to cryptographic keys that have reached the end of their cryptoperiod and include all elements specified in this requirement.	
	3.7.4.b Interview personnel, examine documentation, and observe key storage locations to verify that keys are changed at the end of the defined cryptoperiod(s).	
Customized Approach Objective		
Cryptographic keys are not used beyond their defined cryptoperiod.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Keys that are no longer required, keys with weakened integrity, and keys that are known or suspected to be compromised, should be archived, revoked, and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived encrypted data), they should be strongly protected. **Good Practice** Archived cryptographic keys should be used only for decryption/verification purposes. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan per Requirement 12.10.1. **Further Information** Industry best practices for archiving retired keys are outlined in *NIST SP 800-57 Part 1, Revision 5, Section 8.3.1*, and includes maintaining the archive with a trusted third party and storing archived key information separately from operational data.
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	**3.7.5.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define retirement, replacement, or destruction of keys in accordance with all elements specified in this requirement.	
Customized Approach Objective	**3.7.5.b** Interview personnel to verify that processes are implemented in accordance with all elements specified in this requirement.	
Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.		
Applicability Notes		
If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented, including managing these operations using split knowledge and dual control.	**3.7.6.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define using split knowledge and dual control.	Split knowledge and dual control of keys are used to eliminate the possibility of a single person having access to the whole key and therefore being able to gain unauthorized access to the data.
Customized Approach Objective	**3.7.6.b** Interview personnel and/or observe processes to verify that manual cleartext keys are managed with split knowledge and dual control.	**Definitions**
Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.		Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of other components or of the original cryptographic key. Dual control requires two or more people to authenticate the use of a cryptographic key or perform a key-management function. No single person can access or use the authentication factor (for example, the password, PIN, or key) of another.
Applicability Notes		**Good Practice**
This control is applicable for manual key-management operations. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.		Where key components or key shares are used, procedures should ensure that no single custodian ever has access to sufficient key components or shares to reconstruct the cryptographic key. For example, in an m-of-n scheme (for example, Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian should not then be assigned component B or C, as this would give the custodian knowledge of two components and the ability to recreate the key. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
3.7.6 *(continued)*		**Examples** Key-management operations that might be performed manually include, but are not limited to, key generation, transmission, loading, storage, and destruction. **Further Information** Industry standards for managing key components include: • *NIST SP 800-57* Part 2, Revision 1 -- Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [4.6 Keying Material Distribution] • *ISO 11568-2 Banking — Key management (retail) — Part 2*: Symmetric ciphers, their key management and life cycle [4.7.2.3 Key components and 4.9.3 Key components] • *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [especially 4.1.4 Key installation].
Defined Approach Requirements **3.7.7** Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys. **Customized Approach Objective** Cryptographic keys cannot be substituted by unauthorized personnel.	**Defined Approach Testing Procedures** **3.7.7.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define prevention of unauthorized substitution of cryptographic keys. **3.7.7.b** Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	**Purpose** If an attacker is able to substitute an entity's key with a key the attacker knows, the attacker will be able to decrypt all data encrypted with that key. **Good Practice** The encryption solution should not allow for or accept substitution of keys from unauthorized sources or unexpected processes. Controls should include ensuring that individuals with access to key components or shares do not have access to other components or shares that form the necessary threshold to derive the key.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities. An annual reaffirmation can help remind key custodians of their responsibilities. **Further Information** Industry guidance for key custodians and their roles and responsibilities includes: • *NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems* [5. Roles and Responsibilities (especially) for Key Custodians] • *ISO 11568-1 Banking -- Key management (retail) -- Part 1*: Principles [5 Principles of key management (especially b)]
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	**3.7.8.a** Examine the documented key-management policies and procedures for keys used for protection of stored account data and verify that they define acknowledgments for key custodians in accordance with all elements specified in this requirement.	
	3.7.8.b Examine documentation or other evidence showing that key custodians have provided acknowledgments in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
3.7.9 ***Additional requirement for service providers only:*** Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	**3.7.9** ***Additional testing procedure for service provider assessments only:*** If the service provider shares cryptographic keys with its customers for transmission or storage of account data, examine the documentation that the service provider provides to its customers to verify it includes guidance on how to securely transmit, store, and update customers' keys in accordance with all elements specified in Requirements 3.7.1 through 3.7.8 above.	Providing guidance to customers on how to securely transmit, store, and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities. **Further Information** Numerous industry standards for key management are cited above in the Guidance for Requirements 3.7.1-3.7.8.
Customized Approach Objective		
Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Sections

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.

4.2 PAN is protected with strong cryptography during transmission

Overview

The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.

To protect against compromise, PAN must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). Any transmissions of cardholder data over an entity's internal network(s) will naturally bring that network into scope for PCI DSS since that network stores, processes, or transmits cardholder data. Any such networks must be evaluated and assessed against applicable PCI DSS requirements.

Requirement 4 applies to transmissions of PAN unless specifically called out in an individual requirement.

PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is recommended.

Refer to *Appendix G* for definitions of "strong cryptography" and other PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**4.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 4 are managed in accordance with all elements specified in this requirement.	Requirement 4.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 4. While it is important to define the specific policies or procedures called out in Requirement 4, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	**4.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 4 are documented and assigned.	
	4.1.2.b Interview personnel with responsibility for performing activities in Requirement 4 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
4.2 PAN is protected with strong cryptography during transmission.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit. **Good Practice** The network and data-flow diagrams defined in Requirement 1 are useful resources for identifying all connection points where account data is transmitted or received over open, public networks. While not required, it is considered a good practice for entities to also encrypt PAN over their internal networks, and for entities to establish any new network implementations with encrypted communications. PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both. While it is not required that strong cryptography be applied at both the data level and the session level, it is strongly recommended. If encrypted at the data level, the cryptographic keys used for protecting the data can be managed in accordance with Requirements 3.6 and 3.7. If the data is encrypted at the session level, designated key custodians should be assigned responsibility for managing transmission keys and certificates. *(continued on next page)*
4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	**4.2.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined to include all elements specified in this requirement.	
	4.2.1.b Examine system configurations to verify that strong cryptography and security protocols are implemented in accordance with all elements specified in this requirement.	
	4.2.1.c Examine cardholder data transmissions to verify that all PAN is encrypted with strong cryptography when it is transmitted over open, public networks.	
	4.2.1.d Examine system configurations to verify that keys and/or certificates that cannot be verified as trusted are rejected.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. *The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.*		Some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain access to the cleartext data. It is critical that entities maintain awareness of industry-defined deprecation dates for the cipher suites they are using and are prepared to migrate to newer versions or protocols when older ones are no longer deemed secure. Verifying that certificates are trusted helps ensure the integrity of the secure connection. To be considered trusted, a certificate should be issued from a trusted source, such as a trusted certificate authority (CA), and not be expired. Up-to-date Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used to validate certificates. Techniques to validate certificates may include certificate and public key pinning, where the trusted certificate or a public key is pinned either during development or upon its first use. Entities can also confirm with developers or review source code to ensure that clients and servers reject connections if the certificate is bad. For browser-based TLS certificates, certificate trust can often be verified by clicking on the lock icon that appears next to the address bar. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
4.2.1 *(continued)*		**Examples** Open, public networks include, but are not limited to: • The Internet and • Wireless technologies, including Wi-Fi, Bluetooth, cellular technologies, and satellite communications. **Further Information** Vendor recommendations and industry best practices can be consulted for information about the proper encryption strength specific to the encryption methodology in use. For more information about strong cryptography and secure protocols, see industry standards and best practices such as *NIST SP 800-52* and *SP 800-57*. For more information about trusted keys and certificates, see *NIST Cybersecurity Practice Guide Special Publication 1800-16*, *Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The inventory of trusted keys helps the entity keep track of the algorithms, protocols, key strength, key custodians, and key expiry dates. This enables the entity to respond quickly to vulnerabilities discovered in encryption software, certificates, and cryptographic algorithms. **Good Practice** For certificates, the inventory should include the issuing CA and certification expiration date.
4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	**4.2.1.1.a** Examine documented policies and procedures to verify processes are defined for the entity to maintain an inventory of its trusted keys and certificates.	
	4.2.1.1.b Examine the inventory of trusted keys and certificates to verify it is kept up to date.	
Customized Approach Objective		
All keys and certificates used to protect PAN during transmission are identified and confirmed as trusted.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Since wireless networks do not require physical media to connect, it is important to establish controls limiting who can connect and what transmission protocols will be used. Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks. Wireless networks present unique risks to an organization; therefore, they must be identified and protected according to industry requirements. Strong cryptography for authentication and transmission of PAN is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data. **Good Practice** Wireless networks should not permit fallback or downgrade to an insecure protocol or lower encryption strength that does not meet the intent of strong cryptography. **Further Information** Review the vendor's specific documentation for more details on the choice of protocols, configurations, and settings related to cryptography.
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	**4.2.1.2** Examine system configurations to verify that wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from wireless network transmissions.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** End-user messaging technologies typically can be easily intercepted by packet-sniffing during delivery across internal and public networks. **Good Practice** The use of end-user messaging technology to send PAN should only be considered where there is a defined business need and should be controlled through the Acceptable Use Policies for end-user technologies defined by the entity according to Requirement 12.2.1. **Examples** E-mail, instant messaging, SMS, and chat are examples of the type of end-user messaging technology that this requirement refers to.
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	**4.2.2.a** Examine documented policies and procedures to verify that processes are defined to secure PAN with strong cryptography whenever sent over end-user messaging technologies.	
	4.2.2.b Examine system configurations and vendor documentation to verify that PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	
Customized Approach Objective		
Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.		
Applicability Notes		
This requirement also applies if a customer, or other third party, requests that PAN is sent to them via end-user messaging technologies. There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

Sections	
5.1	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.
5.2	Malicious software (malware) is prevented, or detected and addressed.
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored.
5.4	Anti-phishing mechanisms protect users against phishing attacks.

Overview

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system.

Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.

Malware can enter the network during many business-approved activities, including employee e-mail (for example, via phishing) and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities.

Using anti-malware solutions that address all types of malware helps to protect systems from current and evolving malware threats.

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**5.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 5 are managed in accordance with all elements specified in this requirement.	Requirement 5.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 5. While it is important to define the specific policies or procedures called out in Requirement 5, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	**5.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.	
	5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data. **Good Practice** It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior. **Definitions** System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	**5.2.1.a** Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	
	5.2.1.b For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	
Customized Approach Objective		
Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	
Customized Approach Objective		
Malware cannot execute or infect other system components.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **5.2.3** Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.	**Defined Approach Testing Procedures** **5.2.3.a** Examine documented policies and procedures to verify that a process is defined for periodic evaluations of any system components that are not at risk for malware that includes all elements specified in this requirement. **5.2.3.b** Interview personnel to verify that the evaluations include all elements specified in this requirement. **5.2.3.c** Examine the list of system components identified as not at risk of malware and compare to the system components without an anti-malware solution deployed per Requirement 5.2.1 to verify that the system components match for both requirements.	**Purpose** Certain systems, at a given point in time, may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-malware forums to determine whether its systems might be coming under threat from new and evolving malware. **Good Practice** If an entity determines that a particular system is not susceptible to any malware, the determination should be supported by industry evidence, vendor resources, and best practices. The following steps can help entities during their periodic evaluations: • Identification of all system types previously determined to not require malware protection. • Review of industry vulnerability alerts and notices to determine if new threats exist for any identified system. • A documented conclusion about whether the system types remain not susceptible to malware. • A strategy to add malware protection for any system types for which malware protection has become necessary. Trends in malware should be included in the identification of new security vulnerabilities at Requirement 6.3.1, and methods to address new trends should be incorporated into the entity's configuration standards and protection mechanisms as needed.
Customized Approach Objective The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.		
Applicability Notes System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**5.2.3.1.a** Examine the entity's targeted risk analysis for the frequency of periodic evaluations of system components identified as not at risk for malware to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	Entities determine the optimum period to undertake the evaluation based on criteria such as the complexity of each entity's environment and the number of types of systems that are required to be evaluated.
Customized Approach Objective	**5.2.3.1.b** Examine documented results of periodic evaluations of system components identified as not at risk for malware and interview personnel to verify that evaluations are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	
Systems not known to be at risk from malware are re-evaluated at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	**5.3.1.a** Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution is configured to perform automatic updates.	**Purpose** For an anti-malware solution to remain effective, it needs to have the latest security updates, signatures, threat analysis engines, and any other malware protections on which the solution relies. Having an automated update process avoids burdening end users with responsibility for manually installing updates and provides greater assurance that anti-malware protection mechanisms are updated as quickly as possible after an update is released. **Good Practice** Anti-malware mechanisms should be updated via a trusted source as soon as possible after an update is available. Using a trusted common source to distribute updates to end-user systems helps ensure the integrity and consistency of the solution architecture. Updates may be automatically downloaded to a central location—for example, to allow for testing—prior to being deployed to individual system components.
Customized Approach Objective	**5.3.1.b** Examine system components and logs, to verify that the anti-malware solution(s) and definitions are current and have been promptly deployed	
Anti-malware mechanisms can detect and address the latest malware threats.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Periodic scans can identify malware that is present, but currently inactive, within the environment. Some malware, such as zero-day malware, can enter an environment before the scan solution is capable of detecting it. Performing regular periodic scans or continuous behavioral analysis of systems or processes helps ensure that previously undetectable malware can be identified, removed, and investigated to determine how it gained access to the environment. **Good Practice** Using a combination of periodic scans (scheduled and on-demand) and active, real-time (on-access) scanning helps ensure that malware residing in both static and dynamic elements of the CDE is addressed. Users should also be able to run on-demand scans on their systems if suspicious activity is detected – this can be useful in the early detection of malware. Scans should include the entire file system, including all disks, memory, and start-up files and boot records (at system restart) to detect all malware upon file execution, including any software that may be resident on a system but not currently active. Scan scope should include all systems and software in the CDE, including those that are often overlooked such as email servers, web browsers, and instant messaging software. **Definitions** Active, or real-time, scanning checks files for malware upon any attempt to open, close, rename, or otherwise interact with a file, preventing the malware from being activated.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. **OR** • Performs continuous behavioral analysis of systems or processes.	**5.3.2.a** Examine anti-malware solution(s) configurations, including any master installation of the software, to verify the solution(s) is configured to perform at least one of the elements specified in this requirement.	
	5.3.2.b Examine system components, including all operating system types identified as at risk for malware, to verify the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Customized Approach Objective	**5.3.2.c** Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Malware cannot complete execution.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities can determine the optimum period to undertake periodic scans based on their own assessment of the risks posed to their environments.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**5.3.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic malware scans to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
	5.3.2.1.b Examine documented results of periodic malware scans and interview personnel to verify scans are performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	
Customized Approach Objective		
Scans by the malware solution are performed at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
5.3.3 For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, **OR** • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	**5.3.3.a** Examine anti-malware solution(**s)** configurations to verify that, for removable electronic media, the solution is configured to perform at least one of the elements specified in this requirement.	Portable media devices are often overlooked as an entry method for malware. Attackers will often pre-load malware onto portable devices such as USB and flash drives; connecting an infected device to a computer then triggers the malware, introducing new threats within the environment.
	5.3.3.b Examine system components with removable electronic media connected to verify that the solution(s) is enabled in accordance with at least one of the elements as specified in this requirement.	
Customized Approach Objective	**5.3.3.c** Examine logs and scan results to verify that the solution(s) is enabled in accordance with at least one of the elements specified in this requirement.	
Malware cannot be introduced to system components via external removable media.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	**5.3.4** Examine anti-malware solution(s) configurations to verify logs are enabled and retained in accordance with Requirement 10.5.1.	It is important to track the effectiveness of the anti-malware mechanisms—for example, by confirming that updates and scans are being performed as expected, and that malware is identified and addressed. Audit logs also allow an entity to determine how malware entered the environment and track its activity when inside the entity's network.
Customized Approach Objective		
Historical records of anti-malware actions are immediately available and retained for at least 12 months.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important that defensive mechanisms are always running so that malware is detected in real time. Ad-hoc starting and stopping of anti-malware solutions could allow malware to propagate unchecked and undetected. **Good Practice** Where there is a legitimate need to temporarily disable a system's anti-malware protection—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action should be understood and approved by an appropriate management representative. Any disabling or altering of anti-malware mechanisms, including on administrators' own devices, should be performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable anti-malware on their own computers, but there should be alerting mechanisms in place when such software is disabled and then follow up that occurs to ensure correct processes were followed. **Examples** Additional security measures that may need to be implemented for the period during which anti-malware protection is not active include disconnecting the unprotected system from the Internet while the anti-malware protection is disabled and running a full scan once it is re-enabled.
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	**5.3.5.a** Examine anti-malware configurations, to verify that the anti-malware mechanisms cannot be disabled or altered by users.	
Customized Approach Objective Anti-malware mechanisms cannot be modified by unauthorized personnel.	**5.3.5.b** Interview responsible personnel and observe processes to verify that any requests to disable or alter anti-malware mechanisms are specifically documented and authorized by management on a case-by-case basis for a limited time period.	
Applicability Notes Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
Defined Approach Requirements **5.4.1** Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. **Customized Approach Objective** Mechanisms are in place to protect against and mitigate risk posed by phishing attacks. **Applicability Notes** The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **5.4.1** Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.	**Purpose** Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing. **Good Practice** When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity's domain and impersonating personnel. The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened. It is recommended (but not required) that anti-phishing controls are applied across an entity's entire organization. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
5.4.1 *(continued)*		**Definitions** Phishing is a form of social engineering and describes the different methods used by attackers to trick personnel into disclosing sensitive information, such as user account names and passwords, and account data. Attackers will typically disguise themselves and attempt to appear as a genuine or trusted source, directing personnel to send an email response, click on a web link, or enter data into a compromised website. Mechanisms that can detect and prevent phishing attempts are often included in anti-malware solutions. **Further Information** See the following for more information about phishing: *National Cyber Security Centre - Phishing Attacks: Defending your Organization*. *US Cybersecurity & Infrastructure Security Agency - Report Phishing Sites.*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 6: Develop and Maintain Secure Systems and Software

Sections

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

Overview

Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

Code repositories that store application code, system configurations, or other configuration data that can impact the security of cardholder data and/or sensitive authentication data are in scope for PCI DSS assessments.

See *Relationship between PCI DSS and PCI SSC Software Standards* on page 7 for information about the use of PCI SSC-validated software and software vendors, and how use of PCI SSC's software standards may help with meeting controls in Requirement 6.

Refer to *Appendix G* for definitions of PCI DSS terms.

***Note**: Requirement 6 applies to all system components, except for section 6.2 for developing software securely, which applies only to bespoke and custom software used on any system component included in or connected to the CDE.*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 6.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 6. While it is important to define the specific policies or procedures called out in Requirement 6, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**6.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 6 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	**6.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 6 are documented and assigned.	
	6.1.2.b Interview personnel responsible for performing activities in Requirement 6 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.2 Bespoke and custom software are developed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. **Good Practice** Understanding how sensitive data is handled by the application—including when stored, transmitted, and in memory—can help identify where data needs to be protected. PCI DSS requirements must be considered when developing software to meet those requirements by design, rather than trying to retrofit the software later. **Examples** Secure software lifecycle management methodologies and frameworks include PCI Software Security Framework, BSIMM, OPENSAMM, and works from NIST, ISO, and SAFECode.
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	**6.2.1** Examine documented software development procedures to verify that processes are defined that include all elements specified in this requirement.	
Customized Approach Objective		
Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.		
Applicability Notes		
This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having staff knowledgeable in secure coding methods, including techniques defined in Requirement 6.2.4, will help minimize the number of security vulnerabilities introduced through poor coding practices. **Good Practice** Training for developers may be provided in-house or by third parties. Training should include, but is not limited to, development languages in use, secure software design, secure coding techniques, use of techniques/methods for finding vulnerabilities in code, processes to prevent reintroducing previously resolved vulnerabilities, and how to use any automated security testing tools for detecting vulnerabilities in software. As industry-accepted secure coding practices change, organizational coding practices and developer training may need to be updated to address new threats.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	**6.2.2.a** Examine software development procedures to verify that processes are defined for training of software development personnel developing bespoke and custom software that includes all elements specified in this requirement.	
Customized Approach Objective	**6.2.2.b** Examine training records and interview personnel to verify that software development personnel working on bespoke and custom software received software security training that is relevant to their job function and development languages in accordance with all elements specified in this requirement.	
Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Security vulnerabilities in bespoke and custom software are commonly exploited by malicious individuals to gain access to a network and compromise account data. Vulnerable code is far more difficult and expensive to address after it has been deployed or released into production environments. Requiring a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures. **Good Practice** The following items should be considered for inclusion in code reviews: • Searching for undocumented features (implant tools, backdoors). • Confirming that software securely uses external components' functions (libraries, frameworks, APIs, etc.). For example, if a third-party library providing cryptographic functions is used, verify that it was integrated securely. • Checking for correct use of logging to prevent sensitive data from getting into logs. • Analysis of insecure code structures that may contain potential vulnerabilities related to common software attacks identified in Requirement 6.2.4. • Checking the application's behavior to detect logical vulnerabilities.
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	**6.2.3.a** Examine documented software development procedures and interview responsible personnel to verify that processes are defined that require all bespoke and custom software to be reviewed in accordance with all elements specified in this requirement. **6.2.3.b** Examine evidence of changes to bespoke and custom software to verify that the code changes were reviewed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Bespoke and custom software cannot be exploited via coding vulnerabilities.		
Applicability Notes		
This requirement for code reviews applies to all bespoke and custom software (both internal and public facing), as part of the system development lifecycle. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4. Code reviews may be performed using either manual or automated processes, or a combination of both.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.	**6.2.3.1.a** If manual code reviews are performed for bespoke and custom software prior to release to production, examine documented software development procedures and interview responsible personnel to verify that processes are defined for manual code reviews to be conducted in accordance with all elements specified in this requirement.	Having code reviewed by someone other than the original author, who is both experienced in code reviews and knowledgeable about secure coding practices, minimizes the possibility that code containing security or logic errors that could affect the security of cardholder data is released into a production environment. Requiring management approval that the code was reviewed limits the ability for the process to be bypassed.
Customized Approach Objective	**6.2.3.1.b** Examine evidence of changes to bespoke and custom software and interview personnel to verify that manual code reviews were conducted in accordance with all elements specified in this requirement.	**Good Practice**
The manual code review process cannot be bypassed and is effective at discovering security vulnerabilities.		Having a formal review methodology and review checklists has been found to improve the quality of the code review process. Code review is a tiring process, and for this reason, it is most effective when reviewers only review small amounts of code at a time. To maintain the effectiveness of code reviews, it is beneficial to monitor the general workload of reviewers and to have them review applications they are familiar with. Code reviews may be performed using either manual or automated processes, or a combination of both. Entitles that rely solely on manual code review should ensure that reviewers maintain their skills through regular training as new vulnerabilities are found, and new secure coding methods are recommended.
Applicability Notes		**Further Information**
Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel. An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.		See the *OWASP Code Review Guide*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	**6.2.4** Examine documented procedures and interview responsible software development personnel to verify that software engineering techniques or other methods are defined and in use by developers of bespoke and custom software to prevent or mitigate all common software attacks as specified in this requirement.	**Purpose** Detecting or preventing common errors that result in vulnerable code as early as possible in the software development process lowers the probability that such errors make it through to production and lead to a compromise. Having formal engineering techniques and tools embedded in the development process will catch these errors early. This philosophy is sometimes called "shifting security left." **Good Practice** For both bespoke and custom software, the entity must ensure that code is developed focusing on the prevention or mitigation of common software attacks, including: • Attempts to exploit common coding vulnerabilities (bugs). • Attempts to exploit software design flaws. • Attempts to exploit implementation/configuration flaws. • Enumeration attacks – automated attacks that are actively exploited in payments and abuse identification, authentication, or authorization mechanisms. See the *PCI Perspectives blog article "Beware of Account Testing Attacks*." *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities. **Applicability Notes** This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.		Researching and documenting software engineering techniques or other methods helps to define how software developers prevent or mitigate various software attacks by features or countermeasures they build into software. This might include identification/authentication mechanisms, access control, input validation routines, etc. Developers should be familiar with different types of vulnerabilities and potential attacks and use measures to avoid potential attack vectors when developing code. **Examples** Techniques include automated processes and practices that scan code early in the development cycle when code is checked in to confirm the vulnerabilities are not present.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. *(continued on next page)*
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	
Customized Approach Objective	**6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
New system and software vulnerabilities that may impact the security of cardholder data and/or sensitive authentication data are monitored, cataloged, and risk assessed.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement is not achieved by, and is in addition to, performing vulnerability scans according to Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This process should include multiple sources of vulnerability information, including industry-recognized vulnerability databases (for example, the US National Vulnerability Database), CERTs, RSS feeds, information received from vendors and third parties, and vulnerabilities identified via internal and external vulnerability scans (Requirements 11.3.1 and 11.3.2). This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.3.1 *(continued)*		**Examples** Some organizations that issue alerts to advise entities about urgent vulnerabilities requiring immediate patches/updates are national Computer Emergency Readiness/Response Teams (CERTs) and vendors. Criteria for ranking vulnerabilities may include criticality of a vulnerability identified in an alert from Forum of Incident Response and Security Teams (FIRST) or a CERT, consideration of the CVSS score, the classification by the vendor, and/or type of systems affected. **Further Information** Trustworthy sources for vulnerability information include vendor websites, industry newsgroups, mailing lists, etc. If software is developed in-house, the internal development team should also consider sources of information about new vulnerabilities that may affect internally developed applications. Other methods to ensure new vulnerabilities are identified include solutions that automatically recognize and alert upon detection of unusual behavior. Processes should account for widely published exploits as well as “zero-day” attacks, which target previously unknown vulnerabilities. For bespoke and custom software, the organization may obtain information about libraries, frameworks, compilers, programming languages, etc. from public trusted sources (for example, special resources and resources from component developers). The organization may also independently analyze third-party components and identify vulnerabilities. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.3.1 *(continued)*		For control over in-house developed software, the organization may receive such information from external sources. The organization can consider using a “bug bounty” program where it posts information (for example, on its website) so third parties can contact the organization with vulnerability information. External sources may include independent investigators or companies that report to the organization about identified vulnerabilities and may include sources such as the Common Vulnerability Scoring System (CVSS) or the OWASP Risk Rating Methodology.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Identifying and listing all the entity's bespoke and custom software, and any third-party software that is incorporated into the entity's bespoke and custom software enables the entity to manage vulnerabilities and patches. Vulnerabilities in third-party components (including libraries, APIs, etc.) embedded in an entity's software also renders those applications vulnerable to attacks. Knowing which third-party components are used in the entity's software and monitoring the availability of security patches to address known vulnerabilities is critical to ensuring the security of the software. **Good Practice** An entity's inventory should cover all payment software components and dependencies, including supported execution platforms or environments, third-party libraries, services, and other required functionalities. There are many different types of solutions that can help with managing software inventories, such as software composition analysis tools, application discovery tools, and mobile device management.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	**6.3.2.a** Examine documentation and interview personnel to verify that an inventory of bespoke and custom software and third-party software components incorporated into bespoke and custom software is maintained, and that the inventory is used to identify and address vulnerabilities.	
Customized Approach Objective		
Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.	**6.3.2.b** Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.	
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data. **Good Practice** Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. An entity's patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.	**6.3.3.a** Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.	
	6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
System components cannot be compromised via the exploitation of a known vulnerability.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.3.3 *(continued)*		It is recommended that the entity complete a targeted risk analysis (TRA) according to PCI DSS Requirement 12.3.1 to document the frequency of installing all other applicable security patches/updates. This TRA would include consideration of the entity's assessment of the criticality of the risk to their environment as identified in the risk ranking process at Requirement 6.3.1. **Examples** An example time frame for installation of patches/updates could be 60 days for high-risk vulnerabilities and 90 days for others, as determined by the entity's assessment of risk.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.4 Public-facing web applications are protected against attacks.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections. **OR** • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	**6.4.1** For public-facing web applications, ensure that either one of the required methods is in place as follows: • If manual or automated vulnerability security assessment tools or methods are in use, examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed in accordance with all elements of this requirement specific to the tool/method. **OR** • If an automated technical solution(s) is installed that continually detects and prevents web-based attacks, examine the system configuration settings and audit logs, and interview responsible personnel to verify that the automated technical solution(s) is installed in accordance with all elements of this requirement specific to the solution(s).	**Purpose** Public-facing web applications are those that are available to the public (not only for internal use). These applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. **Good Practice** Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection. When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. **Examples** A web application firewall (WAF) installed in front of public-facing web applications to check all traffic is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective Public-facing web applications are protected against malicious attacks. **Applicability Notes** This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. *This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective.*		Another example of an automated technical solution is Runtime Application Self-Protection (RASP) technologies. When implemented correctly, RASP solutions can detect and block anomalous behavior by the software during execution. While WAFs typically monitor the application perimeter, RASP solutions monitor and block behavior within the application.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. **Good Practice** When using automated technical solutions, it is important to include processes that facilitate timely responses to alerts generated by the solutions so that any detected attacks can be mitigated. Such solutions may also be used to automate mitigation, for example rate-limiting controls, which can be implemented to mitigate against brute-force attacks and enumeration attacks. **Examples** A web application firewall (WAF), which can be either on-premise or cloud-based, installed in front of public-facing web applications to check all traffic, is an example of an automated technical solution that detects and prevents web-based attacks (for example, the attacks included in Requirement 6.2.4). WAFs filter and block non-essential traffic at the application layer. A properly configured WAF helps to prevent application-layer attacks on applications that are improperly coded or configured.
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	**6.4.2** For public-facing web applications, examine the system configuration settings and audit logs, and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks is in place in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Public-facing web applications are protected in real time against malicious attacks.		
Applicability Notes		
This new requirement will replace Requirement 6.4.1 once its effective date is reached. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary.	**6.4.3.a** Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement.	Scripts loaded and executed in the payment page can have their functionality altered without the entity's knowledge and can also have the functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that can read and exfiltrate cardholder data from the consumer browser. Ensuring that the functionality of all such scripts is understood to be necessary for the operation of the payment page minimizes the number of scripts that could be tampered with. Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without appropriate management approval. Where it is impractical for such authorization to occur before a script is changed or a new script is added to the page, the authorization should be confirmed as soon as possible after a change is made. Using techniques to prevent tampering with the script will minimize the probability of the script being modified to carry out unauthorized behavior, such as skimming the cardholder data from the payment page. *(continued on next page)*
Customized Approach Objective	**6.4.3.b** Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.	
Unauthorized code cannot be executed in the payment page as it is rendered in the consumer's browser.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. This requirement also applies to scripts in the entity's webpage(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes). This requirement does not apply to an entity for scripts in a TPSP's/payment processor's embedded payment page/form (for example, one or more iframes), where the entity includes a TPSP's/payment processor's payment page/form on its webpage. Scripts in the TPSP's/payment processor's embedded payment page/form are the responsibility of the TPSP/payment processor to manage in accordance with this requirement. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Good Practice** Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (iframe), restricting the location that the payment page can be loaded from, using the parent page's Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page. Where an entity includes a TPSP's/payment processor's embedded payment page/form on its webpage, the entity should expect the TPSP/payment processor to provide evidence that the TPSP/payment processor is meeting this requirement, in accordance with the TPSP's/payment processor's PCI DSS assessment and Requirement 12.9. **Examples** The integrity of scripts can be enforced by several different mechanisms including, but not limited to: • Sub-resource integrity (SRI), which allows the consumer browser to validate that a script has not been tampered with. • A CSP, which limits the locations the consumer browser can load a script from and transmit account data to. • Proprietary script or tag-management systems, which can prevent malicious script execution.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
6.5 Changes to all system components are managed securely.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Change management procedures must be applied to all changes—including the addition, removal, or modification of any system component—in the production environment. It is important to document the reason for a change and the change description so that relevant parties understand and agree the change is needed. Likewise, documenting the impacts of the change allows all affected parties to plan appropriately for any processing changes. **Good Practice** Approval by authorized parties confirms that the change is legitimate and that the change is sanctioned by the organization. Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Thorough testing by the entity confirms that the security of the environment is not reduced by implementing a change and that all existing security controls either remain in place or are replaced with equal or stronger security controls after the change. The specific testing to be performed will vary according to the type of change and system component(s) affected. For each change, it is important to have documented procedures that address any failures and provide instructions on how to return to a secure state in case the change fails or adversely affects the security of an application or system. These procedures will allow the application or system to be restored to its previous secure state.
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	**6.5.1.a** Examine documented change control procedures to verify procedures are defined for changes to all system components in the production environment to include all elements specified in this requirement.	
	6.5.1.b Examine recent changes to system components and trace those changes back to related change control documentation. For each change examined, verify the change is implemented in accordance with all elements specified in this requirement.	
Customized Approach Objective		
All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **6.5.2** Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. **Customized Approach Objective** All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements. **Applicability Notes** These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.	**Defined Approach Testing Procedures** **6.5.2** Examine documentation for significant changes, interview personnel, and observe the affected systems/networks to verify that the entity confirmed applicable PCI DSS requirements were in place on all new or changed systems and networks and that documentation was updated as applicable.	**Purpose** Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment, and that PCI DSS requirements continue to be met to secure the environment. **Good Practice** Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. **Examples** Applicable PCI DSS requirements that could be impacted include, but are not limited to: • Network and data-flow diagrams are updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—for example, file integrity monitoring (FIM), anti-malware, patches, and audit logging. • Sensitive authentication data is not stored, and all account data storage is documented and incorporated into data retention policy and procedures. • New systems are included in the quarterly vulnerability scanning process. • Systems are scanned for internal and external vulnerabilities after significant changes per Requirements 11.3.1.3 and 11.3.2.1.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Due to the constantly changing state of pre-production environments, they are often less secure than the production environment. **Good Practice** Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications. **Definitions** Pre-production environments include development, testing, user acceptance testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre-production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	**6.5.3.a** Examine policies and procedures to verify that processes are defined for separating the pre-production environment from the production environment via access controls that enforce the separation.	
	6.5.3.b Examine network documentation and configurations of network security controls to verify that the pre-production environment is separate from the production environment(s).	
Customized Approach Objective	**6.5.3.c** Examine access control settings to verify that access controls are in place to enforce separation between the pre-production and production environment(s).	
Pre-production environments cannot introduce risks and vulnerabilities into production environments.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	**6.5.4.a** Examine policies and procedures to verify that processes are defined for separating roles and functions to provide accountability such that only reviewed and approved changes are deployed.	The goal of separating roles and functions between production and pre-production environments is to reduce the number of personnel with access to the production environment and account data and thereby minimize risk of unauthorized, unintentional, or inappropriate access to data and system components and help ensure that access is limited to those individuals with a business need for such access. The intent of this control is to separate critical activities to provide oversight and review to catch errors and minimize the chances of fraud or theft (since two people would need to collude in order to hide an activity). Separating roles and functions, also referred to as separation or segregation of duties, is a key internal control concept to protect an entity's assets.
Customized Approach Objective	**6.5.4.b** Observe processes and interview personnel to verify implemented controls separate roles and functions and provide accountability such that only reviewed and approved changes are deployed.	
Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.		
Applicability Notes		
In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Use of live PANs outside of protected CDEs provides malicious individuals with the opportunity to gain unauthorized access to cardholder data. **Definitions** Live PANs refer to valid PANs (not test PANs) issued by, or on behalf of, a payment brand. Additionally, when payment cards expire, the same PAN is often reused with a different expiry date. All PANs must be verified as being unable to conduct payment transactions or pose fraud risk to the payment system before they are excluded from PCI DSS scope. It is the responsibility of the entity to confirm that PANs are not live.
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	**6.5.5.a** Examine policies and procedures to verify that processes are defined for not using live PANs in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
	6.5.5.b Observe testing processes and interview personnel to verify procedures are in place to ensure live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
Customized Approach Objective	**6.5.5.c** Examine pre-production test data to verify live PANs are not used in pre-production environments, except where those environments are in a CDE and protected in accordance with all applicable PCI DSS requirements.	
Live PANs cannot be present in pre-production environments outside the CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This data may give away information about the functioning of an application or system and is an easy target for unauthorized individuals to exploit to gain access to systems. Possession of such information could facilitate compromise of the system and related account data.
6.5.6 Test data and test accounts are removed from system components before the system goes into production.	**6.5.6.a** Examine policies and procedures to verify that processes are defined for removal of test data and test accounts from system components before the system goes into production.	
	6.5.6.b Observe testing processes for both off-the-shelf software and in-house applications, and interview personnel to verify test data and test accounts are removed before a system goes into production.	
Customized Approach Objective	**6.5.6.c** Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications to verify there is no test data or test accounts on systems in production.	
Test data and test accounts cannot exist in production environments.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

Sections	
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.
7.2	Access to system components and data is appropriately defined and assigned.
7.3	Access to system components and data is managed via an access control system(s).

Overview

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Access” or “access rights” are created by rules that provide users access to systems, applications, and data, while “privileges” allow a user to perform a specific action or function in relation to that system, application, or data. For example, a user may have access rights to specific data, but whether they can only read that data, or can also change or delete the data is determined by the user’s assigned privileges.

“Need to know” refers to providing access to only the least amount of data needed to perform a job.

“Least privileges” refers to providing only the minimum level of privileges needed to perform a job.

These requirements apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties (for example, for providing support or maintenance services). Certain requirements also apply to application and system accounts used by the entity (also called “service accounts”).

These requirements do not apply to consumers (cardholders).

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**7.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 7 are managed in accordance with all elements specified in this requirement.	Requirement 7.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 7. While it is important to define the specific policies or procedures called out in Requirement 7, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	**7.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 7 are documented and assigned.	
	7.1.2.b Interview personnel with responsibility for performing activities in Requirement 7 to verify that roles and responsibilities are assigned as and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
7.2 Access to system components and data is appropriately defined and assigned.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Defining an access control model that is appropriate for the entity's technology and access control philosophy supports a consistent and uniform way of allocating access and reduces the possibility of errors such as the granting of excessive rights. **Good Practice** A factor to consider when defining access needs is the separation of duties principle. This principle is intended to prevent fraud and misuse or theft of resources. For example, 1) dividing mission-critical functions and information system support functions among different individuals and/or functions, 2) establishing roles such that information system support activities are performed by different functions/individuals (for example, system management, programming, configuration management, quality assurance and testing, and network security), and 3) ensuring security personnel administering access control functions do not also administer audit functions. In environments where one individual performs multiple functions, such as administration and security operations, duties may be assigned so that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals. *(continued on next page)*
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	**7.2.1.a** Examine documented policies and procedures and interview personnel to verify the access control model is defined in accordance with all elements specified in this requirement.	
	7.2.1.b Examine access control model settings and verify that access needs are appropriately defined in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Access requirements are established according to job functions following least-privilege and need-to-know principles.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
7.1.2 *(continued)*		**Definitions** Key elements of an access control model include: • Resources to be protected (the systems/devices/data to which access is needed), • Job functions that need access to the resource (for example, system administrator, call-center personnel, store clerk), and • Which activities each job function needs to perform (for example, read/write or query). Once job functions, resources, and activities per job functions are defined, individuals can be granted access accordingly. **Examples** Access control models that entities can consider include role-based access control (RBAC) and attribute-based access control (ABAC). The access control model used by a given entity depends on their business and access needs.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID. **Good Practice** Access rights are granted to a user by assignment to one or several functions. Access is assigned depending on the specific user functions and with the minimum scope required for the job. When assigning privileged access, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Once needs are defined for user functions (per PCI DSS requirement 7.2.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles. Entities may wish to consider use of Privileged Access Management (PAM), which is a method to grant access to privileged accounts only when those privileges are required, immediately revoking that access once they are no longer needed.
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	**7.2.2.a** Examine policies and procedures to verify they cover assigning access to users in accordance with all elements specified in this requirement.	
	7.2.2.b Examine user access settings, including for privileged users, and interview responsible management personnel to verify that privileges assigned are in accordance with all elements specified in this requirement.	
Customized Approach Objective	**7.2.2.c** Interview personnel responsible for assigning access to verify that privileged user access is assigned in accordance with all elements specified in this requirement.	
Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.
7.2.3 Required privileges are approved by authorized personnel.	**7.2.3.a** Examine policies and procedures to verify they define processes for approval of all privileges by authorized personnel.	
	7.2.3.b Examine user IDs and assigned privileges, and compare with documented approvals to verify that: • Documented approval exists for the assigned privileges. • The approval was by authorized personnel. • Specified privileges match the roles assigned to the individual.	
Customized Approach Objective		
Access privileges cannot be granted to users without appropriate, documented authorization.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regular review of access rights helps to detect excessive access rights remaining after user job responsibilities change, system functions change, or other modifications. If excessive user rights are not revoked in due time, they may be used by malicious users for unauthorized access. This review provides another opportunity to ensure that accounts for all terminated users have been removed (if any were missed at the time of termination), as well as to ensure that any third parties that no longer need access have had their access terminated. **Good Practice** When a user transfers into a new role or a new department, typically the privileges and access associated with their former role are no longer required. Continued access to privileges or functions that are no longer required may introduce the risk of misuse or errors. Therefore, when responsibilities change, processes that revalidate access help to ensure user access is appropriate for the user's new responsibilities. Entities can consider implementing a regular, repeatable process for conducting reviews of access rights, and assigning "data owners" that are responsible for managing and monitoring access to data related to their job function and that also ensure user access remains current and appropriate. As an example, a direct manager could review team access monthly, while the senior manager reviews their groups' access quarterly, both making updates to access as needed. The intent of these best practices is to support and facilitate conducting the reviews at least once every 6 months.
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	**7.2.4.a** Examine policies and procedures to verify they define processes to review all user accounts and related access privileges, including third-party/vendor accounts, in accordance with all elements specified in this requirement.	
Customized Approach Objective	**7.2.4.b** Interview responsible personnel and examine documented results of periodic reviews of user accounts to verify that all the results are in accordance with all elements specified in this requirement.	
Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.		
Applicability Notes		
This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **7.2.5** All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. **Customized Approach Objective** Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **7.2.5.a** Examine policies and procedures to verify they define processes to manage and assign application and system accounts and related access privileges in accordance with all elements specified in this requirement. **7.2.5.b** Examine privileges associated with system and application accounts and interview responsible personnel to verify that application and system accounts and related access privileges are assigned and managed in accordance with all elements specified in this requirement.	**Purpose** It is important to establish the appropriate access level for application or system accounts. If such accounts are compromised, malicious users will receive the same access level as that granted to the application or system. Therefore, it is important to ensure limited access is granted to system and application accounts on the same basis as to user accounts. **Good Practice** Entities may want to consider establishing a baseline when setting up these application and system accounts including the following as applicable to the organization: • Making sure that the account is not a member of a privileged group such as domain administrators, local administrators, or root. • Restricting which computers the account can be used on. • Restricting hours of use. • Removing any additional settings like VPN access and remote access.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	**7.2.5.1.a** Examine policies and procedures to verify they define processes to review all application and system accounts and related access privileges in accordance with all elements specified in this requirement.	Regular review of access rights helps to detect excessive access rights remaining after system functions change, or other application or system modifications occur. If excessive rights are not removed when no longer needed, they may be used by malicious users for unauthorized access.
Customized Approach Objective	**7.2.5.1.b** Examine the entity's targeted risk analysis for the frequency of periodic reviews of application and system accounts and related access privileges to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
Application and system account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.	**7.2.5.1.c** Interview responsible personnel and examine documented results of periodic reviews of system and application accounts and related privileges to verify that the reviews occur in accordance with all elements specified in this requirement.	
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **7.2.6** All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD. **Customized Approach Objective** Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator. **Applicability Notes** This requirement applies to controls for user access to query repositories of stored cardholder data. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.	**Defined Approach Testing Procedures** **7.2.6.a** Examine policies and procedures and interview personnel to verify processes are defined for granting user access to query repositories of stored cardholder data, in accordance with all elements specified in this requirement. **7.2.6.b** Examine configuration settings for querying repositories of stored cardholder data to verify they are in accordance with all elements specified in this requirement.	**Purpose** The misuse of query access to repositories of cardholder data has been a regular cause of data breaches. Limiting such access to administrators reduces the risk of such access being abused by unauthorized users. **Definitions** "Programmatic methods" means granting access through means such as database stored procedures that allow users to perform controlled actions to data in a table, rather than via direct, unfiltered access to the data repository by end users (except for the responsible administrator(s), who need direct access to the database for their administrative duties). **Good Practice** Typical user actions include moving, copying, and deleting data. Also consider the scope of privilege needed when granting access. For example, access can be granted to specific objects such as data elements, files, tables, indexes, views, and stored routines. Granting access to repositories of cardholder data should follow the same process as all other granted access, meaning that it is based on roles, with only the privileges assigned to each user that are needed to perform their job functions.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
7.3 Access to system components and data is managed via an access control system(s).		
Defined Approach Requirements **7.3.1** An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. **Customized Approach Objective** Access rights and privileges are managed via mechanisms intended for that purpose.	**Defined Approach Testing Procedures** **7.3.1** Examine vendor documentation and system settings to verify that access is managed for each system component via an access control system(s) that restricts access based on a user's need to know and covers all system components.	**Purpose** Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges.
Defined Approach Requirements **7.3.2** The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. **Customized Approach Objective** Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.	**Defined Approach Testing Procedures** **7.3.2** Examine vendor documentation and system settings to verify that the access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	**Purpose** Restricting privileged access with an access control system reduces the opportunity for errors in the assignment of permissions to individuals, applications, and systems.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A default setting of “deny all” ensures no one is granted access unless a rule is established specifically granting such access. **Good Practice** It is important to check the default configuration of access control systems because some are set by default to “allow all,” thereby permitting access unless/until a rule is written to specifically deny it.
7.3.3 The access control system(s) is set to “deny all” by default.	**7.3.3** Examine vendor documentation and system settings to verify that the access control system(s) is set to “deny all” by default.	
Customized Approach Objective		
Access rights and privileges are prohibited unless expressly permitted.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 8: Identify Users and Authenticate Access to System Components

Sections

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

Overview

Two fundamental principles of identifying and authenticating users are to 1) establish the identity of an individual or process on a computer system, and 2) prove or verify the user associated with the identity is who the user claims to be.

Identification of an individual or process on a computer system is conducted by associating an identity with a person or process through an identifier, such as a user, system, or application ID. These IDs (also referred to as "accounts") fundamentally establish the identity of an individual or process by assigning unique identification to each person or process to distinguish one user or process from another. When each user or process can be uniquely identified, it ensures there is accountability for actions performed by that identity. When such accountability is in place, actions taken can be traced to known and authorized users and processes.

The element used to prove or verify the identity is known as the authentication factor. Authentication factors are 1) something you know, such as a password or passphrase, 2) something you have, such as a token device or smart card, or 3) something you are, such as a biometric element.

The ID and the authentication factor together are considered authentication credentials and are used to gain access to the rights and privileges associated with a user, application, system, or service accounts.

These requirements for identity and authentication are based on industry-accepted security principles and best practices to support the payment ecosystem. *NIST Special Publication 800-63, Digital Identity Guidelines* provides additional information on acceptable frameworks for digital identity and authentication factors. It is important to note that the *NIST Digital Identity Guidelines* is intended for US Federal Agencies and should be viewed in its entirety. Many of the concepts and approaches defined in these guidelines are expected to work with each other and not as standalone parameters.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

***Note**: Unless otherwise stated in the requirement, these requirements apply to **all accounts on all system components**, unless specifically called out in an individual requirement, including but not limited to:*

- *Point-of-sale accounts*
- *Accounts with administrative capabilities*
- *System and application accounts*
- *All accounts used to view or access cardholder data or to access systems with cardholder data.*

This includes accounts used by employees, contractors, consultants, internal and external vendors, and other third parties (for example, for providing support or maintenance services).

Certain requirements are not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. When items do not apply, they are noted directly within the specific requirement.

These requirements do not apply to accounts used by consumers (cardholders).

Refer to Appendix G for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 8.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 8. While it is important to define the specific policies or procedures called out in Requirement 8, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**8.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures that are identified in Requirement 8 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	**8.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 8 are documented and assigned.	
	8.1.2.b Interview personnel with responsibility for performing activities in Requirement 8 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	**8.2.1.a** Interview responsible personnel to verify that all users are assigned a unique ID for access to system components and cardholder data.	The ability to trace actions performed on a computer system to an individual establishes accountability and traceability and is fundamental to establishing effective access controls. By ensuring each user is uniquely identified, instead of using one ID for several employees, an organization can maintain individual responsibility for actions and an effective record in the audit log per employee. In addition, this will assist with issue resolution and containment when misuse or malicious intent occurs.
Customized Approach Objective	**8.2.1.b** Examine audit logs and other evidence to verify that access to system components and cardholder data can be uniquely identified and associated with individuals.	
All actions by all users are attributable to an individual.		
Applicability Notes		
This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.2.2 Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • ID use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	**8.2.2.a** Examine user account lists on system components and applicable documentation to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement. **8.2.2.b** Examine authentication policies and procedures to verify processes are defined for shared authentication credentials such that they are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement. **8.2.2.c** Interview system administrators to verify that shared authentication credentials are only used when necessary, on an exception basis, and are managed in accordance with all elements specified in this requirement.	Group, shared, or generic (or default) IDs are typically delivered with software or operating systems—for example, root or with privileges associated with a specific function, such as an administrator. If multiple users share the same authentication credentials (for example, user ID and password), it becomes impossible to trace system access and activities to an individual. In turn, this prevents an entity from assigning accountability for, or having effective logging of, an individual's actions since a given action could have been performed by anyone in the group with knowledge of the user ID and associated authentication factors. The ability to associate individuals to the actions performed with an ID is essential to provide individual accountability and traceability regarding who performed an action, what action was performed, and when that action occurred. **Good Practice** If shared IDs are used for any reason, strong management controls need to be established to maintain individual accountability and traceability. *(continued on next page)*
Customized Approach Objective		
All actions performed by users with group, shared, or generic IDs are attributable to an individual person.		
Applicability Notes		
This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.2.2 *(continued)*		**Examples** Tools and techniques can facilitate both management and security of these types of accounts and confirm individual user identity before access to an account is granted. Entities can consider password vaults or other system-managed controls such as the *sudo* command. An example of an exceptional circumstance is where all other authentication methods have failed, and a shared ID is needed for emergency use or "break the glass" administrator access.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.2.3 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises. **Customized Approach Objective** A service provider's credential used for one customer cannot be used for any other customer.	**8.2.3** ***Additional testing procedure for service provider assessments only:*** Examine authentication policies and procedures and interview personnel to verify that service providers with remote access to customer premises use unique authentication factors for remote access to each customer premises.	Service providers with remote access to customer premises typically use this access to support POS POI systems or provide other remote services. If a service provider uses the same authentication factors to access multiple customers, all the service provider's customers can easily be compromised if an attacker compromises that one factor. Criminals know this and deliberately target service providers looking for a shared authentication factor that gives them remote access to many merchants via that single factor. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider. This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted. If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Requirement 8.2.2.		**Examples** Technologies such as multi-factor mechanisms that provide a unique credential for each connection (such as a single-use password) could also meet the intent of this requirement.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	**8.2.4** Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions) and examine system settings to verify the activity has been managed in accordance with all elements specified in this requirement.	It is imperative that the lifecycle of a user ID (additions, deletions, and modifications) is controlled so that only authorized accounts can perform functions, actions are auditable, and privileges are limited to only what is required. Attackers often compromise an existing account and then escalate the privileges of that account to perform unauthorized acts, or they may create new IDs to continue their activity in the background. It is essential to detect and respond when user IDs are created or changed outside the normal change process or without corresponding authorization.
Customized Approach Objective		
Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.		
Applicability Notes		
This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.2.5 Access for terminated users is immediately revoked.	**8.2.5.a** Examine information sources for terminated users and review current user access lists—for both local and remote access—to verify that terminated user IDs have been deactivated or removed from the access lists.	If an employee or third party/vendor has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account.
Customized Approach Objective	**8.2.5.b** Interview responsible personnel to verify that all physical authentication factors—such as, smart cards, tokens, etc.—have been returned or deactivated for terminated users.	
The accounts of terminated users cannot be used.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Accounts that are not used regularly are often targets of attack since it is less likely that any changes, such as a changed password, will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data. **Good Practice** Where it may be reasonably anticipated that an account will not be used for an extended period of time, such as an extended leave of absence, the account should be disabled as soon as the leave begins, rather than waiting 90 days.
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity. **Customized Approach Objective** Inactive user accounts cannot be used.	**8.2.6** Examine user accounts and last logon information, and interview personnel to verify that any inactive user accounts are removed or disabled within 90 days of inactivity.	
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Allowing third parties to have 24/7 access into an entity's systems and networks in case they need to provide support increases the chances of unauthorized access. This access could result in an unauthorized user in the third party's environment or a malicious individual using the always-available external entry point into an entity's network. Where third parties do need access 24/7, it should be documented, justified, monitored, and tied to specific service reasons. *(continued on next page)*
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	**8.2.7** Interview personnel, examine documentation for managing accounts, and examine evidence to verify that accounts used by third parties for remote access are managed according to all elements specified in this requirement.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective Third-party remote access cannot be used except where specifically authorized and use is overseen by management.		**Good Practice** Enabling access only for the time periods needed and disabling it as soon as it is no longer required helps prevent misuse of these connections. Additionally, consider assigning third parties a start and stop date for their access in accordance with their service contract. Monitoring third-party access helps ensure that third parties are accessing only the systems necessary and only during approved time frames. Any unusual activity using third-party accounts should be followed up and resolved.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. **Good Practice** The re-authentication can be applied either at the system level to protect all sessions running on that machine or at the application level. Entities may also want to consider staging controls in succession to further restrict the access of an unattended session as time passes. For example, the screensaver may activate after 15 minutes and log off the user after an hour. However, timeout controls must balance the risk of access and exposure with the impact to the user and purpose of the access. If a user needs to run a program from an unattended computer, the user can log in to the computer to initiate the program, and then "lock" the computer so that no one else can use the user's login while the computer is unattended. **Examples** One way to meet this requirement is to configure an automated screensaver to launch whenever the console is idle for 15 minutes and requiring the logged-in user to enter their password to unlock the screen.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	**8.2.8** Examine system configuration settings to verify that system/session idle timeout features for user sessions have been set to 15 minutes or less.	
Customized Approach Objective		
A user session cannot be used except by the authorized user.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.3 Strong authentication for users and administrators is established and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	**8.3.1.a** Examine documentation describing the authentication factor(s) used to verify that user access to system components is authenticated via at least one authentication factor specified in this requirement.	When used in addition to unique IDs, an authentication factor helps protect user IDs from being compromised, since the attacker needs to have the unique ID and compromise the associated authentication factor(s). **Good Practice** A common approach for a malicious individual to compromise a system is to exploit weak or nonexistent authentication factors (for example, passwords/passphrases). Requiring strong authentication factors helps protect against this attack. **Further Information** See *fidoalliance.org* for more information about using tokens, smart cards, or biometrics as authentication factors.
Customized Approach Objective	**8.3.1.b** For each type of authentication factor used with each type of system component, observe an authentication to verify that authentication is functioning consistently with documented authentication factor(s).	
An account cannot be accessed except with a combination of user identity and an authentication factor.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for “something you have” if it is unique for a particular user.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Network devices and applications have been known to transmit unencrypted, readable authentication factors (such as passwords and passphrases) across the network and/or store these values without encryption. As a result, a malicious individual can easily intercept this information during transmission using a "sniffer," or directly access unencrypted authentication factors in files where they are stored, and then use this data to gain unauthorized access.
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	**8.3.2.a** Examine vendor documentation and system configuration settings to verify that authentication factors are rendered unreadable with strong cryptography during transmission and storage.	
	8.3.2.b Examine repositories of authentication factors to verify that they are unreadable during storage.	
	8.3.2.c Examine data transmissions to verify that authentication factors are unreadable during transmission.	
Customized Approach Objective		
Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals use "social engineering" techniques to impersonate a user of a system — for example, calling a help desk and acting as a legitimate user—to have an authentication factor changed so they can use a valid user ID. Requiring positive identification of a user reduces the probability of this type of attack succeeding. **Good Practice** Modifications to authentication factors for which user identity should be verified include but are not limited to performing password resets, provisioning new hardware or software tokens, and generating new keys. **Examples** Methods to verify a user's identity include a secret question/answer, knowledge-based information, and calling the user back at a known and previously established phone number.
8.3.3 User identity is verified before modifying any authentication factor. **Customized Approach Objective** Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.	**8.3.3** Examine procedures for modifying authentication factors and observe security personnel to verify that when a user requests a modification of an authentication factor, the user's identity is verified before the authentication factor is modified.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **8.3.4** Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. **Customized Approach Objective** An authentication factor cannot be guessed in a brute force, online attack. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	**Defined Approach Testing Procedures** **8.3.4.a** Examine system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than 10 invalid logon attempts. **8.3.4.b** Examine system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until the user's identity is confirmed.	**Purpose** Without account-lockout mechanisms in place, an attacker can continually try to guess a password through manual or automated tools (for example, password cracking) until the attacker succeeds and gains access to a user's account. If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of the locked account stop the malicious individual from guessing the password, as they will have to stop for a minimum of 30 minutes until the account is reactivated. **Good Practice** Before reactivating a locked account, the user's identity should be confirmed. For example, the administrator or help desk personnel can validate that the actual account owner is requesting reactivation, or there may be password reset self-service mechanisms that the account owner uses to verify their identity.
Defined Approach Requirements **8.3.5** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use. **Customized Approach Objective** An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.	**Defined Approach Testing Procedures** **8.3.5** Examine procedures for setting and resetting passwords/passphrases (if used as authentication factors to meet Requirement 8.3.1) and observe security personnel to verify that passwords/passphrases are set and reset in accordance with all elements specified in this requirement.	**Purpose** If the same password/passphrase is used for every new user, an internal user, former employee, or malicious individual may know or easily discover the value and use it to gain access to accounts before the authorized user attempts to use the password.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Strong passwords/passphrases may be the first line of defense into a network since a malicious individual will often first try to find accounts with weak, static, or non-existent passwords. If passwords are short or easily guessable, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. **Good Practice** Password/passphrase strength is dependent on password/passphrase complexity, length, and randomness. Passwords/passphrases should be sufficiently complex, so they are impractical for an attacker to guess or otherwise discover its value. Entities can consider adding increased complexity by requiring the use of special characters and upper- and lower-case characters, in addition to the minimum standards outlined by this requirement. Additional complexity increases the time required for offline brute force attacks of hashed passwords/passphrases. Another option for increasing the resistance of passwords to guessing attacks is by comparing proposed password/passphrases to a bad password list and having users provide new passwords for any passwords found on the list.
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	**8.3.6** Examine system configuration settings to verify that user password/passphrase complexity parameters are set in accordance with all elements specified in this requirement.	
Customized Approach Objective A guessed password/passphrase cannot be verified by either an online or offline brute force attack.		
Applicability Notes This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • Application or system accounts, which are governed by requirements in section 8.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	**8.3.7** Examine system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases.	If password history is not maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period reduces the likelihood that passwords that have been guessed or brute-forced will be re-used in the future. Passwords or passphrases may have previously been changed due to suspicion of compromise or because the password or passphrase exceeded its effective use period, both of which are reasons why previously used passwords should not be reused.
Customized Approach Objective		
A previously used password cannot be used to gain access to an account for at least 12 months.		
Applicability Notes		
This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Communicating authentication policies and procedures to all users helps them to understand and abide by the policies. **Good Practice** Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that do not contain dictionary words or information about the user, such as the user ID, names of family members, date of birth, etc. Guidance for protecting authentication factors may include not writing down passwords or not saving them in insecure files, and being alert to malicious individuals who may try to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Alternatively, entities can implement processes to confirm passwords meet password policy, for example, by comparing password choices to a list of unacceptable passwords and having users choose a new password for any that match with one on the list. Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	**8.3.8.a** Examine procedures and interview personnel to verify that authentication policies and procedures are distributed to all users.	
	8.3.8.b Review authentication policies and procedures that are distributed to users and verify they include the elements specified in this requirement.	
Customized Approach Objective	**8.3.8.c** Interview users to verify that they are familiar with authentication policies and procedures.	
Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Access to in-scope system components that are not in the CDE may be provided using a single authentication factor, such as a password/passphrase, token device or smart card, or biometric attribute. Where passwords/passphrases are employed as the only authentication factor for such access, additional controls are required to protect the integrity of the password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password. Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. *(continued on next page)*
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**8.3.9** If passwords/passphrases are used as the only authentication factor for user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	
Customized Approach Objective		
An undetected compromised password/passphrase cannot be used indefinitely.		
Applicability Notes		
This requirement does not apply to in-scope system components where MFA is used. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.3.9 *(continued)*		Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points, which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that authentication credentials have been compromised. **Further Information** For information about using dynamic analysis to manage user access to resources, see *NIST SP 800-207 Zero Trust Architecture*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password.
8.3.10 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	**8.3.10** ***Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data, examine guidance provided to customer users to verify that the guidance includes all elements specified in this requirement.	
Customized Approach Objective		
Passwords/passphrases for service providers' customers cannot be used indefinitely.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. *This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effective.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using a password/passphrase as the only authentication factor provides a single point of failure if compromised. Therefore, in these implementations, controls are needed to minimize how long malicious activity could occur via a compromised password/passphrase. **Good Practice** Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to break the password/phrase. Periodically changing passwords offers less time for a malicious individual to crack a password/passphrase and less time to use a compromised password. Dynamically analyzing an account's security posture is another option that allows for more rapid detection and response to address potentially compromised credentials. Such analysis takes a number of data points which may include device integrity, location, access times, and the resources accessed to determine in real time whether an account can be granted access to a requested resource. In this way, access can be denied and accounts blocked if it is suspected that account credentials have been compromised. **Further Information** For information about using dynamic analysis to manage user access to resources, refer to *NIST SP 800-207 Zero Trust Architecture*.
8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**8.3.10.1** ***Additional testing procedure for service provider assessments only:*** If passwords/passphrases are used as the only authentication factor for customer user access, inspect system configuration settings to verify that passwords/passphrases are managed in accordance with ONE of the elements specified in this requirement.	
Customized Approach Objective		
Passwords/passphrases for service providers' customers cannot be used indefinitely.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	**8.3.11.a** Examine authentication policies and procedures to verify that procedures for using authentication factors such as physical security tokens, smart cards, and certificates are defined and include all elements specified in this requirement.	**Purpose** If multiple users can use authentication factors such as tokens, smart cards, and certificates, it may be impossible to identify the individual using the authentication mechanism. **Good Practice** Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely authenticate the user of the account will prevent unauthorized users from gaining access to the user account through use of a shared authentication factor.
	8.3.11.b Interview security personnel to verify authentication factors are assigned to an individual user and not shared among multiple users.	
Customized Approach Objective	**8.3.11.c** Examine system configuration settings and/or observe physical controls, as applicable, to verify that controls are implemented to ensure only the intended user can use that factor to gain access.	
An authentication factor cannot be used by anyone other than the user to which it is assigned.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	**8.4.1.a** Examine network and/or system configurations to verify MFA is required for all non-console into the CDE for personnel with administrative access.	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase. **Good Practice** Implementing MFA for non-console administrative access to in-scope system components that are not part of the CDE will help prevent unauthorized users from using a single factor to gain access and compromise in-scope system components. **Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.
Customized Approach Objective	**8.4.1.b** Observe administrator personnel logging into the CDE and verify that MFA is required.	
Administrative access to the CDE cannot be obtained by the use of a single authentication factor.		
Applicability Notes		
The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase. *(continued on next page)*
8.4.2 MFA is implemented for all non-console access into the CDE.	**8.4.2.a** Examine network and/or system configurations to verify MFA is implemented for all non-console access into the CDE.	
	8.4.2.b Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.	
Customized Approach Objective		
Access into the CDE cannot be obtained by the use of a single authentication factor.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • User accounts that are only authenticated with phishing-resistant authentication factors. MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting from the entity's network into the CDE. *(continued on next page)*		**Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. Refer to *Appendix G* for the definition of "phishing resistant authentication."

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. MFA for access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows, such as a password or passphrase. **Definitions** Multi-factor authentication (MFA) requires an individual to present a minimum of two of the three authentication factors specified in Requirement 8.3.1 before access is granted. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. *(continued on next page)*
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.	**8.4.3.a** Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement.	
	8.4.3.b Observe personnel (for example, users and administrators) and third parties connecting remotely to the network and verify that multi-factor authentication is required.	
Customized Approach Objective		
Remote access to the entity's network cannot be obtained by using a single authentication factor.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers). If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	**8.5.1.a** Examine vendor system documentation to verify that the MFA system is not susceptible to replay attacks. **8.5.1.b** Examine system configurations for the MFA implementation to verify it is configured in accordance with all elements specified in this requirement. **8.5.1.c** Interview responsible personnel and observe processes to verify that any requests to bypass MFA are specifically documented and authorized by management on an exception basis, for a limited time period. **8.5.1.d** Observe personnel logging into system components in the CDE to verify that access is granted only after all authentication factors are successful. **8.5.1.e** Observe personnel connecting remotely from outside the entity's network to verify that access is granted only after all authentication factors are successful.	**Purpose** Poorly configured MFA systems can be bypassed by attackers. This requirement therefore addresses configuration of MFA system(s) that provide MFA for users accessing system components in the CDE. **Definitions** Using one type of factor twice (for example, using two separate passwords) is not considered multi-factor authentication. A replay attack is when an attacker intercepts a valid transmission of data and then resends or redirects this communication for malicious purposes. In MFA implementations, replay attacks are typically used to gain unauthorized access by leveraging legitimate credentials. **Examples** Examples of methods to help protect against replay attacks include, but are not limited to: • Unique session identifiers and session keys • Timestamps • Time-based, one-time passwords or passcodes • Anti-replay mechanisms that detect and reject duplicated authentication attempts. *(continued on next page)*
Customized Approach Objective		
MFA systems are resistant to attack and strictly control any administrative overrides.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Further Information** For more information about MFA systems and features, refer to the following: PCI SSC's *Information Supplement: Multi-Factor Authentication* PCI SSC's Frequently Asked Questions (FAQs) on this topic.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.6 Use of application and system accounts and associated authentication factors is strictly managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Like individual user accounts, system and application accounts require accountability and strict management to ensure they are used only for the intended purpose and are not misused. Attackers often compromise system or application accounts to gain access to cardholder data. **Good Practice** Where possible, configure system and application accounts to disallow interactive login to prevent unauthorized individuals from logging in and using the account with its associated system privileges, and to limit the machines and devices on which the account can be used. **Definitions** Interactive login is the ability for a person to log into a system or application account in the same manner as a normal user account. Using system and application accounts this way means there is no accountability and traceability of actions taken by the user. Refer to *Appendix G* for the definition of "application and system accounts."
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	**8.6.1** Examine application and system accounts that can be used interactively and interview administrative personnel to verify that application and system accounts are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Not properly protecting passwords/passphrases used by application and system accounts, especially if those accounts can be used for interactive login, increases the risk and success of unauthorized use of those privileged accounts. **Good Practice** Changing these values due to suspected or confirmed disclosure can be particularly difficult to implement. Tools can facilitate both management and security of authentication factors for application and system accounts. For example, consider password vaults or other system-managed controls.
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	**8.6.2.a** Interview personnel and examine system development procedures to verify that processes are defined for application and system accounts that can be used for interactive login, specifying that passwords/passphrases are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	
	8.6.2.b Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login, to verify passwords/passphrases for those accounts are not present.	
Customized Approach Objective Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.		
Applicability Notes Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Systems and application accounts pose more inherent security risk than user accounts because they often run in an elevated security context, with access to systems that may not be typically granted to user accounts, such as programmatic access to databases, etc. As a result, special consideration must be made to protect passwords/passphrases used for application and system accounts. **Good Practice** Entities should consider the following risk factors when determining how to protect application and system passwords/passphrases against misuse: • How securely the passwords/passphrases are stored (for example, whether they are stored in a password vault). • Staff turnover. • The number of people with access to the authentication factor. • Whether the account can be used for interactive login. • Whether the security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly (see Requirement 8.3.9). All these elements affect the level of risk for application and system accounts and might impact the security of systems accessed by the system and application accounts. *(continued on next page)*
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	**8.6.3.a** Examine policies and procedures to verify that procedures are defined to protect passwords/passphrases for application or system accounts against misuse in accordance with all elements specified in this requirement.	
	8.6.3.b Examine the entity's targeted risk analysis for the change frequency and complexity for passwords/passphrases for application and system accounts to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1 and addresses: • The frequency defined for periodic changes to application and system passwords/passphrases. • The complexity defined for passwords/passphrases and appropriateness of the complexity relative to the frequency of changes.	
Customized Approach Objective Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.	**8.6.3.c** Interview responsible personnel and examine system configuration settings to verify that passwords/passphrases for any application and system accounts are protected against misuse in accordance with all elements specified in this requirement.	
Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
8.6.3 *(continued)*		Entities should correlate their selected change frequency for application and system passwords/passwords with their selected complexity for those passwords/passphrases – i.e., the complexity should be more rigorous when passwords/passphrases are changed infrequently and can be less rigorous when changed more frequently. For example, a longer change frequency is more justifiable when passwords/passphrases complexity is set to 36 alphanumeric characters with upper- and lower-case letters, numbers, and special characters. Best practices are to consider password changes at least once a year, a password/passphrase length of at least 15 characters, and complexity for the passwords/passphrase of alphanumeric characters, with upper- and lower-case letters, and special characters. **Further Information** For information about variability and equivalency of password strength for passwords/passphrases of different formats, see the industry standards (for example, the current version of *NIST SP 800-63 Digital Identity Guidelines*).

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9: Restrict Physical Access to Cardholder Data

Sections

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

Overview

Any physical access to cardholder data or systems that store, process, or transmit cardholder data provides the opportunity for individuals to access and/or remove systems or hardcopies containing cardholder data; therefore, physical access should be appropriately restricted.

There are three different areas mentioned in Requirement 9:

1. Requirements that specifically refer to sensitive areas are intended to apply to those areas only. Each entity should identify the sensitive areas in its environments to ensure the appropriate physical controls are implemented.
2. Requirements that specifically refer to the cardholder data environment (CDE) are intended to apply to the entire CDE, including any sensitive areas residing within the CDE.
3. Requirements that specifically refer to the facility are referencing the types of controls that may be managed more broadly at the physical boundary of a business premise (such as a building) within which CDEs and sensitive areas reside. These controls often exist outside a CDE or sensitive area, for example a guard desk that identifies, badges, and logs visitors. The term “facility” is used to recognize that these controls may exist at different places within a facility, for instance, at building entry or at an internal entrance to a data center or office space.

Refer to *Appendix G* for definitions of “media,” “personnel,” “sensitive areas,” “visitors,” and other PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**9.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 9 are managed in accordance with all elements specified in this requirement.	Requirement 9.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 9. While it is important to define the specific policies or procedures called out in Requirement 9, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives. Policies and procedures, including updates, are actively communicated to all affected personnel, and are supported by operating procedures describing how to perform activities.
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	**9.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 9 are documented and assigned.	
	9.1.2.b Interview personnel with responsibility for performing activities in Requirement 9 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without physical access controls, unauthorized persons could potentially gain access to the CDE and sensitive information, or could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment. Therefore, the purpose of this requirement is that physical access to the CDE is controlled via physical security controls such as badge readers or other mechanisms such as lock and key. **Good Practice** Whichever mechanism meets this requirement, it must be sufficient for the organization to verify that only authorized personnel are granted access. **Examples** Facility entry controls include physical security controls at each computer room, data center, and other physical areas with systems in the CDE. It can also include badge readers or other devices that manage physical access controls, such as lock and key with a current list of all individuals holding the keys.
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. **Customized Approach Objective** System components in the CDE cannot be physically accessed by unauthorized personnel. **Applicability Notes** This requirement does not apply to locations that are publicly accessible by consumers (cardholders).	**9.2.1** Observe entry controls and interview responsible personnel to verify that physical security controls are in place to restrict access to systems in the CDE.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining details of individuals entering and exiting the sensitive areas can help with investigations of physical breaches by identifying individuals that physically accessed the sensitive areas, as well as when they entered and exited. **Good Practice** Whichever mechanism meets this requirement, it should effectively monitor all entry and exit points to sensitive areas. Criminals attempting to gain physical access to sensitive areas will often try to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, physical access control mechanisms could be monitored or have physical protections installed to prevent them from being damaged or disabled by malicious individuals.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	**9.2.1.1.a** Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are in place to monitor the entry and exit points.	
	9.2.1.1.b Observe locations where individual physical access to sensitive areas within the CDE occurs to verify that either video cameras or physical access control mechanisms (or both) are protected from tampering or disabling.	
Customized Approach Objective	**9.2.1.1.c** Observe the physical access control mechanisms and/or examine video cameras and interview responsible personnel to verify that: • Collected data from video cameras and/or physical access control mechanisms is reviewed and correlated with other entries. • Collected data is stored for at least three months.	
Trusted, verifiable records are maintained of individual physical entry to, and exit from, sensitive areas.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **9.2.2** Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. **Customized Approach Objective** Unauthorized devices cannot connect to the entity's network from public areas within the facility.	**Defined Approach Testing Procedures** **9.2.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks within the facility.	**Purpose** Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gaining access to the CDE or systems connected to the CDE. **Good Practice** Whether logical or physical controls, or a combination of both, are used, they should prevent an individual or device that is not explicitly authorized from being able to connect to the network. **Examples** Methods to meet this requirement include network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.
Defined Approach Requirements **9.2.3** Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. **Customized Approach Objective** Physical networking equipment cannot be accessed by unauthorized personnel.	**Defined Approach Testing Procedures** **9.2.3** Interview responsible personnel and observe locations of hardware and lines to verify that physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	**Purpose** Without appropriate physical security over access to wireless components and devices, and computer networking and telecommunications equipment and lines, malicious users could gain access to the entity's network resources. Additionally, they could connect their own devices to the network to gain unauthorized access to the CDE or systems connected to the CDE. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	**9.2.4** Observe a system administrator's attempt to log into consoles in sensitive areas and verify that they are "locked" to prevent unauthorized use.	Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.
Customized Approach Objective		
Physical consoles within sensitive areas cannot be used by unauthorized personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.3 Physical access for personnel and visitors is authorized and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	**9.3.1.a** Examine documented procedures to verify that procedures to authorize and manage physical access of personnel to the CDE are defined in accordance with all elements specified in this requirement.	**Purpose** Establishing procedures for granting, managing, and removing access when it is no longer needed ensures non-authorized individuals are prevented from gaining access to areas containing cardholder data. In addition, it is important to limit access to the actual badging system and badging materials to prevent unauthorized personnel from making their own badges and/or setting up their own access rules. **Good Practice** It is important to visually identify the personnel that are physically present, and whether the individual is a visitor or an employee. **Definitions** Refer to *Appendix G* for the definition of "personnel." **Examples** One way to identify personnel is to assign them badges.
	9.3.1.b Observe identification methods, such as ID badges, and processes to verify that personnel in the CDE are clearly identified.	
Customized Approach Objective	**9.3.1.c** Observe processes to verify that access to the identification process, such as a badge system, is limited to authorized personnel.	
Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Controlling physical access to sensitive areas helps ensure that only authorized personnel with a legitimate business need are granted access. **Good Practice** Where possible, organizations should have policies and procedures to ensure that before personnel leaving the organization, all physical access mechanisms are returned, or disabled as soon as possible upon their departure. This will ensure personnel cannot gain physical access to sensitive areas once their employment has ended.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	**9.3.1.1.a** Observe personnel in sensitive areas within the CDE, interview responsible personnel, and examine physical access control lists to verify that: • Access to the sensitive area is authorized. • Access is required for the individual's job function.	
	9.3.1.1.b Observe processes and interview personnel to verify that access of all personnel is revoked immediately upon termination.	
Customized Approach Objective	**9.3.1.1.c** For terminated personnel, examine physical access controls lists and interview responsible personnel to verify that all physical access mechanisms (such as keys, access cards, etc.) were returned or disabled.	
Sensitive areas cannot be accessed by unauthorized personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	**9.3.2.a** Examine documented procedures and interview personnel to verify procedures are defined for authorizing and managing visitor access to the CDE in accordance with all elements specified in this requirement.	**Purpose** Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities and potentially to cardholder data. Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit. **Definitions** Refer to *Appendix G* for the definition of "visitor."
	9.3.2.b Observe processes when visitors are present in the CDE and interview personnel to verify that visitors are: • Authorized before entering the CDE. • Escorted at all times within the CDE.	
	9.3.2.c Observe the use of visitor badges or other identification to verify that the badge or other identification does not permit unescorted access to the CDE.	
	9.3.2.d Observe visitors in the CDE to verify that: • Visitor badges or other identification are being used for all visitors. • Visitor badges or identification easily distinguish visitors from personnel.	
Customized Approach Objective	**9.3.2.e** Examine visitor badges or other identification and observe evidence in the badging system to verify visitor badges or other identification expires.	
Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility and interview personnel to verify visitor badges or other identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. upon departure or expiration.	Ensuring that visitor badges are returned or deactivated upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended.
Customized Approach Objective		
Visitor identification or badges cannot be reused after expiration.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.3.4 Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	**9.3.4.a** Examine the visitor logs and interview responsible personnel to verify that visitor logs are used to record physical access to both the facility and sensitive areas. **9.3.4.b** Examine the visitor logs and verify that the logs contain: • The visitor's name and the organization represented. • The personnel authorizing physical access. • Date and time of visit. **9.3.4.c** Examine visitor log storage locations and interview responsible personnel to verify that the log is retained for at least three months, unless otherwise restricted by law.	A visitor log documenting minimum information about the visitor is easy and inexpensive to maintain. It will assist in identifying historical physical access to a building or room and potential access to cardholder data. **Good Practice** When logging the date and time of visit, including both in and out times is considered a best practice, since it provides helpful tracking information and provides assurance that a visitor has left at the end of the day. It is also good to verify that a visitor's ID (driver's license, etc.) matches the name they put on the visitor log.
Customized Approach Objective		
Records of visitor access that enable the identification of individuals are maintained.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.4.1 All media with cardholder data is physically secured.	**9.4.1.** Examine documentation to verify that the procedures defined for protecting cardholder data include controls for physically securing all media.	Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk.
Customized Approach Objective		
Media with cardholder data cannot be accessed by unauthorized personnel.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	**9.4.1.1.a** Examine documentation to verify that procedures are defined for physically securing offline media backups with cardholder data in a secure location.	If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent. **Good Practice** For secure storage of backup media, a good practice is to store media in an off-site facility, such as an alternate or backup site or commercial storage facility.
Customized Approach Objective	**9.4.1.1.b** Examine logs or other documentation and interview responsible personnel at the storage location to verify that offline media backups are stored in a secure location.	
Offline backups cannot be accessed by unauthorized personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Conducting regular reviews of the storage facility enables the organization to address identified security issues promptly, minimizing the potential risk. It is important for the entity to be aware of the security of the area where media is being stored.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	**9.4.1.2.a** Examine documentation to verify that procedures are defined for reviewing the security of the offline media backup location(s) with cardholder data at least once every 12 months.	
	9.4.1.2.b Examine documented procedures, logs, or other documentation, and interview responsible personnel at the storage location(s) to verify that the storage location's security is reviewed at least once every 12 months.	
Customized Approach Objective		
The security controls protecting offline backups are verified periodically by inspection.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Media not identified as confidential may not be adequately protected or may be lost or stolen. **Good Practice** It is important that media be identified such that its classification status is apparent. This does not mean however that the media needs to have a "confidential" label.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	**9.4.2.a** Examine documentation to verify that procedures are defined for classifying media with cardholder data in accordance with the sensitivity of the data.	
	9.4.2.b Examine media logs or other documentation to verify that all media is classified in accordance with the sensitivity of the data.	
Customized Approach Objective		
Media are classified and protected appropriately.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	**9.4.3.a** Examine documentation to verify that procedures are defined for securing media sent outside the facility in accordance with all elements specified in this requirement.	Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. The use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.
	9.4.3.b Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.	
Customized Approach Objective	**9.4.3.c** Examine offsite tracking logs for all media to verify tracking details are documented.	
Media is secured and tracked when transported outside the facility.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **9.4.4** Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). **Customized Approach Objective** Media cannot leave a facility without the approval of accountable personnel. **Applicability Notes** Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have “manager” as part of their title.	**Defined Approach Testing Procedures** **9.4.4.a** Examine documentation to verify that procedures are defined to ensure that media moved outside the facility is approved by management. **9.4.4.b** Examine offsite media tracking logs and interview responsible personnel to verify that proper management authorization is obtained for all media moved outside the facility (including media distributed to individuals).	**Purpose** Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.
Defined Approach Requirements **9.4.5** Inventory logs of all electronic media with cardholder data are maintained. **Customized Approach Objective** Accurate inventories of stored electronic media are maintained.	**Defined Approach Testing Procedures** **9.4.5.a** Examine documentation to verify that procedures are defined to maintain electronic media inventory logs. **9.4.5.b** Examine electronic media inventory logs and interview responsible personnel to verify that logs are maintained.	**Purpose** Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	**9.4.5.1.a** Examine documentation to verify that procedures are defined to conduct inventories of electronic media with cardholder data at least once every 12 months.	Without careful inventory methods and storage controls, stolen or missing electronic media could go unnoticed for an indefinite amount of time.
Customized Approach Objective	**9.4.5.1.b** Examine electronic media inventory logs and interview personnel to verify that electronic media inventories are performed at least once every 12 months.	
Media inventories are verified periodically.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	**9.4.6.a** Examine the media destruction policy to verify that procedures are defined to destroy hard-copy media with cardholder data when no longer needed for business or legal reasons in accordance with all elements specified in this requirement. **9.4.6.b** Observe processes and interview personnel to verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that cardholder data cannot be reconstructed. **9.4.6.c** Observe storage containers used for materials that contain information to be destroyed to verify that the containers are secure.	If steps are not taken to destroy information contained on hard-copy media before disposal, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for hard-copy materials with information they can use to launch an attack. Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. **Good Practice** Consider "to-be-shredded" containers with a lock that prevents access to its contents or that physically prevent access to the inside of the container. **Further Information** See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*.
Customized Approach Objective		
Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.		
Applicability Notes		
These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **9.4.7** Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed. **Customized Approach Objective** Cardholder data cannot be recovered from media that has been erased or destroyed. **Applicability Notes** These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.	**Defined Approach Testing Procedures** **9.4.7.a** Examine the media destruction policy to verify that procedures are defined to destroy electronic media when no longer needed for business or legal reasons in accordance with all elements specified in this requirement. **9.4.7.b** Observe the media destruction process and interview responsible personnel to verify that electronic media with cardholder data is destroyed via one of the methods specified in this requirement.	**Purpose** If steps are not taken to destroy information contained on electronic media when no longer needed, malicious individuals may retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack. **Good Practice** The deletion function in most operating systems allows deleted data to be recovered, so instead, a dedicated secure deletion function or application should be used to make data unrecoverable. **Examples** Methods for securely destroying electronic media include secure wiping in accordance with industry-accepted standards for secure deletion, degaussing, or physical destruction (such as grinding or shredding hard disks). **Further Information** See *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	**9.5.1** Examine documented policies and procedures to verify that processes are defined that include all elements specified in this requirement.	Criminals attempt to steal payment card data by stealing and/or manipulating card-reading devices and terminals. Criminals will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card data every time a card is entered. They will also try to add "skimming" components to the outside of devices, which are designed to capture payment card data before it enters the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card data is captured twice: once by the criminal's component and then by the device's legitimate component. In this way, transactions may still be completed without interruption while the criminal is "skimming" the payment card data during the process.
Customized Approach Objective		
The entity has defined procedures to protect and manage point-of-interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). These requirements do not apply to: • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.		*(continued on next page)* **Good Practice** Entities may consider implementing protection from tampering and unauthorized substitution for: • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution. **Further Information** Additional best practices on skimming prevention are available on the PCI SSC website.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Keeping an up-to-date list of POI devices helps an organization track where devices are supposed to be and quickly identify if a device is missing or lost. *(continued on next page)*
9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	**9.5.1.1.a** Examine the list of POI devices to verify it includes all elements specified in this requirement. **9.5.1.1.b** Observe POI devices and device locations and compare to devices in the list to verify that the list is accurate and up to date.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective The identity and location of POI devices is recorded and known at all times.	**9.5.1.1.c** Interview personnel to verify the list of POI devices is updated when devices are added, relocated, decommissioned, etc.	**Good Practice** The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned. **Examples** Methods to maintain device locations include identifying the address of the site or facility where the device is located.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regular inspections of devices will help organizations detect tampering more quickly via external evidence—for example, the addition of a card skimmer—or replacement of a device, thereby minimizing the potential impact of using fraudulent devices. **Good Practice** Methods for periodic inspection include checking the serial number or other device characteristics and comparing the information to the list of POI devices to verify the device has not been swapped with a fraudulent device. *(continued on next page)*
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	**9.5.1.2.a** Examine documented procedures to verify processes are defined for periodic inspections of POI device surfaces to detect tampering and unauthorized substitution.	
	9.5.1.2.b Interview responsible personnel and observe inspection processes to verify: • Personnel are aware of procedures for inspecting devices. • All devices are periodically inspected for evidence of tampering and unauthorized substitution.	
Customized Approach Objective		
Point of interaction devices cannot be tampered with, substituted without authorization, or have skimming attachments installed without timely detection.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.5.1.2 *(continued)*		**Examples** The type of inspection will depend on the device. For instance, photographs of devices known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also provide security guidance and "how to" guides to help determine whether the device has been subject to tampering. Signs that a device might have been tampered with or substituted include: • Unexpected attachments or cables plugged into the device. • Missing or changed security labels. • Broken or differently colored casing. • Changes to the serial number or other external markings.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities are best placed to determine the frequency of POI device inspections based on the environment in which the device operates. **Good Practice** The frequency of inspections will depend on factors such as the location of a device and whether the device is attended or unattended. For example, devices left in public areas without supervision by the organization's personnel might have more frequent inspections than devices kept in secure areas or supervised when accessible to the public. In addition, many POI vendors include guidance in their user documentation about how often POI devices should be checked, and for what – entities should consult their vendors' documentation and incorporate those recommendations into their periodic inspections.
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	**9.5.1.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic POI device inspections and type of inspections performed to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1.	
	9.5.1.2.1.b Examine documented results of periodic device inspections and interview personnel to verify that the frequency and type of POI device inspections performed match what is defined in the entity's targeted risk analysis conducted for this requirement.	
Customized Approach Objective		
POI devices are inspected at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Criminals will often pose as authorized maintenance personnel to gain access to POI devices. **Good Practice** Personnel training should include being alert to and questioning anyone who shows up to do POI maintenance to ensure they are authorized and have a valid work order, including any agents, maintenance or repair personnel, technicians, service providers, or other third parties. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POI maintenance company, such as the vendor or acquirer, for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work apparel), and could also be knowledgeable about locations of devices, so personnel should be trained to always follow procedures. Another trick that criminals use is to send a "new" POI device with instructions for swapping it with a legitimate device and "returning" the legitimate device. The criminals may even provide return postage to their specified address. Therefore, personnel should always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business. *(continued on next page)*
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	**9.5.1.3.a** Review training materials for personnel in POI environments to verify they include all elements specified in this requirement. **9.5.1.3.b** Interview personnel in POI environments to verify they have received training and know the procedures for all elements specified in this requirement.	
Customized Approach Objective		
Personnel are knowledgeable about the types of attacks against POI devices, the entity's technical and procedural countermeasures, and can access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
9.5.1.3 *(continued)*		**Examples** Suspicious behavior that personnel should be aware of includes attempts by unknown persons to unplug or open devices. Ensuring personnel are aware of mechanisms for reporting suspicious behavior and who to report such behavior to—for example, a manager or security officer—will help reduce the likelihood and potential impact of a device being tampered with or substituted.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Sections

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Overview

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

This requirement applies to user activities, including those by employees, contractors, consultants, and internal and external vendors, and other third parties (for example, those providing support or maintenance services).

These requirements do not apply to user activity of consumers (cardholders).

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 10.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 10. While it is important to define the specific policies or procedures called out in Requirement 10, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**10.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 10 are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	**10.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 10 are documented and assigned.	
	10.1.2.b Interview personnel with responsibility for performing activities in Requirement 10 to verify that roles and responsibilities are assigned as defined and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
Defined Approach Requirements **10.2.1** Audit logs are enabled and active for all system components and cardholder data. **Customized Approach Objective** Records of all activities affecting system components and cardholder data are captured.	**Defined Approach Testing Procedures** **10.2.1** Interview the system administrator and examine system configurations to verify that audit logs are enabled and active for all system components.	**Purpose** Audit logs must exist for all system components. Audit logs send alerts the system administrator, provides data to other monitoring mechanisms, such as intrusion-detection systems (IDS) and security information and event monitoring systems (SIEM) tools, and provide a history trail for post-incident investigation. Logging and analyzing security-relevant events enable an organization to identify and trace potentially malicious activities. **Good Practice** When an entity considers which information to record in their logs, it is important to remember that information stored in audit logs is sensitive and should be protected per requirements in this standard. Care should be taken to only store essential information in the audit logs to minimize risk.
Defined Approach Requirements **10.2.1.1** Audit logs capture all individual user access to cardholder data. **Customized Approach Objective** Records of all individual user access to cardholder data are captured.	**Defined Approach Testing Procedures** **10.2.1.1** Examine audit log configurations and log data to verify that all individual user access to cardholder data is logged.	**Purpose** It is critical to have a process or system that links user access to system components accessed. Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account to access cardholder data. **Good Practice** A record of all individual access to cardholder data can identify which accounts may have been compromised or misused.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **10.2.1.2** Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. **Customized Approach Objective** Records of all actions performed by individuals with elevated privileges are captured.	**Defined Approach Testing Procedures** **10.2.1.2** Examine audit log configurations and log data to verify that all actions taken by any individual with administrative access, including any interactive use of application or system accounts, are logged.	**Purpose** Accounts with increased access privileges, such as the "administrator" or "root" account, have the potential to significantly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is cannot trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and account. **Definitions** The functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions. Refer to *Appendix G* for the definition of "administrative access."
Defined Approach Requirements **10.2.1.3** Audit logs capture all access to audit logs. **Customized Approach Objective** Records of all access to audit logs are captured.	**Defined Approach Testing Procedures** **10.2.1.3** Examine audit log configurations and log data to verify that access to all audit logs is captured.	**Purpose** Malicious users often attempt to alter audit logs to hide their actions. A record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having logs identify changes, additions, and deletions to the audit logs can help retrace steps made by unauthorized personnel.
Defined Approach Requirements **10.2.1.4** Audit logs capture all invalid logical access attempts.	**Defined Approach Testing Procedures**	**Purpose** Malicious individuals will often perform multiple access attempts on targeted systems. Multiple

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective Records of all invalid access attempts are captured.	**10.2.1.4** Examine audit log configurations and log data to verify that invalid logical access attempts are captured.	invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Logging changes to authentication credentials (including elevation of privileges, additions, and deletions of accounts with administrative access) provides residual evidence of activities. Malicious users may attempt to manipulate authentication credentials to bypass them or impersonate a valid account.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	**10.2.1.5** Examine audit log configurations and log data to verify that changes to identification and authentication credentials are captured in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Records of all changes to identification and authentication credentials are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Turning off or pausing audit logs before performing illicit activities is common practice for malicious users who want to avoid detection. Initialization of audit logs could indicate that that a user disabled the log function to hide their actions.
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	**10.2.1.6** Examine audit log configurations and log data to verify that all elements specified in this requirement are captured.	
Customized Approach Objective		
Records of all changes to audit log activity status are captured.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	**10.2.1.7** Examine audit log configurations and log data to verify that creation and deletion of system level objects is captured.	Malicious software, such as malware, often creates or replaces system-level objects on the target system to control a particular function or operation on that system. By logging when system-level objects are created or deleted, it will be easier to determine whether such modifications were authorized.
Customized Approach Objective		
Records of alterations that indicate a system has been modified from its intended functionality are captured.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	**10.2.2** Interview personnel and examine audit log configurations and log data to verify that all elements specified in this requirement are included in log entries for each auditable event (from 10.2.1.1 through 10.2.1.7).	By recording these details for the auditable events at 10.2.1.1 through 10.2.1.7, a potential compromise can be quickly identified, with sufficient detail to facilitate following up on suspicious activities.
Customized Approach Objective		
Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.3 Audit logs are protected from destruction and unauthorized modifications.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Audit log files contain sensitive information, and read access to the log files must be limited only to those with a valid business need. This access includes audit log files on the originating systems as well as anywhere else they are stored. **Good Practice** Adequate protection of the audit logs includes strong access control that limits access to logs based on “need to know” only and the use of physical or network segregation to make the logs harder to find and modify.
10.3.1 Read access to audit logs files is limited to those with a job-related need. **Customized Approach Objective** Stored activity records cannot be accessed by unauthorized personnel.	**10.3.1** Interview system administrators and examine system configurations and privileges to verify that only individuals with a job-related need have read access to audit log files.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Often a malicious individual who has entered the network will try to edit the audit logs to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise. Therefore, audit logs should be protected on the originating systems as well as anywhere else they are stored. **Good Practice** Entities should attempt to prevent logs from being exposed in public-accessible locations.
10.3.2 Audit log files are protected to prevent modifications by individuals. **Customized Approach Objective** Stored activity records cannot be modified by personnel.	**10.3.2** Examine system configurations and privileges and interview system administrators to verify that current audit log files are protected from modifications by individuals via access control mechanisms, physical segregation, and/or network segregation.	
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected, even if the system generating the logs becomes compromised. Writing logs from external-facing technologies such as wireless, network security controls, DNS, and mail servers, reduces the risk of those logs being lost or altered. **Good Practice** Each entity determines the best way to back up log files, whether via one or more centralized log servers or other secure media. Logs may be written directly, offloaded, or copied from external systems to the secure internal system or media.
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. **Customized Approach Objective** Stored activity records are secured and preserved in a central location to prevent unauthorized modification.	**10.3.3** Examine backup configurations or log files to verify that current audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** File integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are identified. For file integrity monitoring purposes, an entity usually monitors files that do not regularly change, but when changed, indicate a possible compromise. **Good Practice** Software used to monitor changes to audit logs should be configured to provide alerts when existing log data or files are changed or deleted. However, new log data being added to an audit log should not generate an alert.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	**10.3.4** Examine system settings, monitored files, and results from monitoring activities to verify the use of file integrity monitoring or change-detection software on audit logs.	
Customized Approach Objective		
Stored activity records cannot be modified without an alert being generated.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Many breaches occur months before being detected. Regular log reviews mean incidents can be quickly identified and proactively addressed. **Good Practice** Checking logs daily (7 days a week, 365 days a year, including holidays) minimizes the amount of time and exposure of a potential breach. Log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions are examples of automated tools that can be used to meet this requirement. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file integrity monitoring (FIM) systems, etc., is necessary to identify potential issues. The determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior. An entity that uses third-party service providers to perform log review services is responsible to provide context about the entity's environment to the service providers, so it understands the entity's environment, has a baseline of "normal" traffic for the entity, and can detect potential security issues and provide accurate exceptions and anomaly notifications.
10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	**10.4.1.a** Examine security policies and procedures to verify that processes are defined for reviewing all elements specified in this requirement at least once daily.	
	10.4.1.b Observe processes and interview personnel to verify that all elements specified in this requirement are reviewed at least once daily	
Customized Approach Objective		
Potentially suspicious or anomalous activities are quickly identified to minimize impact.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed. **Good Practice** Establishing a baseline of normal audit activity patterns is critical to the effectiveness of an automated log review mechanism. The analysis of new audit activity against the established baseline can significantly improve the identification of suspicious or anomalous activities. The entity should keep logging tools aligned with any changes in their environment by periodically reviewing tool settings and updating settings to reflect any changes. **Further Information** Refer to the Information Supplement: *Effective Daily Log Monitoring* for additional guidance.
10.4.1.1 Automated mechanisms are used to perform audit log reviews. **Customized Approach Objective** Potentially suspicious or anomalous activities are identified via a repeatable and consistent mechanism. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**10.4.1.1** Examine log review mechanisms and interview personnel to verify that automated mechanisms are used to perform log reviews.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	**10.4.2.a** Examine security policies and procedures to verify that processes are defined for reviewing logs of all other system components periodically.	Periodic review of logs for all other system components (not specified in Requirement 10.4.1) helps to identify indications of potential issues or attempts to access critical systems via less-critical systems.
	10.4.2.b Examine documented results of log reviews and interview personnel to verify that log reviews are performed periodically.	
Customized Approach Objective		
Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.		
Applicability Notes		
This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Entities can determine the optimum period to review these logs based on criteria such as the complexity of each entity's environment, the number of types of systems that are required to be evaluated, and the functions of such systems.
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	**10.4.2.1.a** Examine the entity's targeted risk analysis for the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	
Customized Approach Objective	**10.4.2.1.b** Examine documented results of periodic log reviews of all other system components (not defined in Requirement 10.4.1) and interview personnel to verify log reviews are performed at the frequency specified in the entity's targeted risk analysis performed for this requirement.	
Log reviews for lower-risk system components are performed at a frequency that addresses the entity's risk.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="4">Purpose
If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities occurring within their network.
Good Practice
Entities should consider how to address the following when developing their processes for defining and managing exceptions and anomalies:
• How log review activities are recorded,
• How to rank and prioritize exceptions and anomalies,
• What procedures should be in place to report and escalate exceptions and anomalies, and
• Who is responsible for investigating and for any remediation tasks.</td></tr>
<tr><td rowspan="2">10.4.3 Exceptions and anomalies identified during the review process are addressed.</td><td>10.4.3.a Examine security policies and procedures to verify that processes are defined for addressing exceptions and anomalies identified during the review process.</td></tr>
<tr><td rowspan="2">10.4.3.b Observe processes and interview personnel to verify that, when exceptions and anomalies are identified, they are addressed.</td></tr>
<tr><td>Customized Approach Objective

Suspicious or anomalous activities are addressed.</td></tr>
</table>

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.5 Audit log history is retained and available for analysis.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Retaining historical audit logs for at least 12 months is necessary because compromises often go unnoticed for significant lengths of time. Having centrally stored log history allows investigators to better determine the length of time a potential breach was occurring, and the possible system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. **Examples** Methods that allow logs to be immediately available include storing logs online, archiving logs, or restoring logs quickly from backups.
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	**10.5.1.a** Examine documentation to verify that the following is defined: • Audit log retention policies. • Procedures for retaining audit log history for at least 12 months, with at least the most recent three months immediately available online.	
	10.5.1.b Examine configurations of audit log history, interview personnel and examine audit logs to verify that audit logs history is retained for at least 12 months.	
Customized Approach Objective	**10.5.1.c** Interview personnel and observe processes to verify that at least the most recent three months' audit log history is immediately available for analysis.	
Historical records of activity are available immediately to support incident response and are retained for at least 12 months.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of events, which is crucial for forensic analysis following a breach. For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity are critical in determining how the systems were compromised. **Examples** Network Time Protocol (NTP) is one example of time-synchronization technology.
10.6.1 System clocks and time are synchronized using time-synchronization technology.	**10.6.1** Examine system configuration settings to verify that time-synchronization technology is implemented and kept current.	
Customized Approach Objective		
Common time is established across all systems.		
Applicability Notes		
Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Using reputable time servers is a critical component of the time synchronization process. Accepting time updates from specific, industry-accepted external sources helps prevent a malicious individual from changing time settings on systems. **Good Practice** Another option to prevent unauthorized use of internal time servers is to encrypt updates with a symmetric key and create access control lists that specify the IP addresses of client machines that will be provided with the time updates.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	**10.6.2** Examine system configuration settings for acquiring, distributing, and storing the correct time to verify the settings are configured in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The time on all systems is accurate and consistent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Attackers will try to change time configurations to hide their activity. Therefore, restricting the ability to change or modify time synchronization configurations or the system time to administrators will lessen the probability of an attacker successfully changing time configurations.
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	**10.6.3.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need.	
	10.6.3.b Examine system configurations and time synchronization settings and logs and observe processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.	
Customized Approach Objective		
System time settings cannot be modified by unauthorized personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE. **Good Practice** The specific types of failures may vary, depending on the function of the device system component and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner, such as a firewall erasing all its rules or going offline.
10.7.1 ***Additional requirement for service providers only:*** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	**10.7.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	
Customized Approach Objective	**10.7.1.b** ***Additional testing procedure for service provider assessments only:*** Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	
Failures in critical security control systems are promptly identified and addressed.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. *This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise system components and steal account data from the CDE. **Good Practice** The specific types of failures may vary, depending on the function of the device system component and technology in use. However, typical failures include a system no longer performing its security function or not functioning in its intended manner—for example, a firewall erasing its rules or going offline.
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	**10.7.2.a** Examine documentation to verify that processes are defined for the prompt detection and addressing of failures of critical security control systems, including but not limited to failure of all elements specified in this requirement.	
	10.7.2.b Observe detection and alerting processes and interview personnel to verify that failures of critical security control systems are detected and reported, and that failure of a critical security control results in the generation of an alert.	
Customized Approach Objective		
Failures in critical security control systems are promptly identified and addressed.		
Applicability Notes		
This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. **Good Practice** Documented evidence (for example, records within a problem management system) should provide support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
10.7.3 Failures of any critical security control systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	**10.7.3.a** Examine documentation and interview personnel to verify that processes are defined and implemented to respond to a failure of any critical security control system and include at least all elements specified in this requirement.	
	10.7.3.b Examine records to verify that failures of critical security control systems are documented to include: • Identification of cause(s) of the failure. • Duration (date and time start and end) of the security failure. • Details of the remediation required to address the root cause.	
Customized Approach Objective		
Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities. *This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 11:Test Security of Systems and Networks Regularly

Sections

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

Overview

Vulnerabilities are being discovered continually by malicious individuals and researchers, as well as being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requirement 11.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 11. While it is important to define the specific policies or procedures called out in Requirement 11, it is equally important to ensure they are properly documented, maintained, and disseminated. **Good Practice** It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. **Definitions** Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	**11.1.1** Examine documentation and interview personnel to verify that security policies and operational procedures are managed in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Expectations, controls, and oversight for meeting activities within Requirement 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	**11.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 11 are documented and assigned.	
	11.1.2.b Interview personnel with responsibility for performing activities in Requirement 11 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	**11.2.1.a** Examine policies and procedures to verify processes are defined for managing both authorized and unauthorized wireless access points with all elements specified in this requirement. **11.2.1.b** Examine the methodology(ies) in use and the resulting documentation, and interview personnel to verify processes are defined to detect and identify both authorized and unauthorized wireless access points in accordance with all elements specified in this requirement. **11.2.1.c** Examine wireless assessment results and interview personnel to verify that wireless assessments were conducted in accordance with all elements specified in this requirement. **11.2.1.d** If automated monitoring is used, examine configuration settings to verify the configuration will generate alerts to notify personnel.	Implementation and/or exploitation of wireless technology within a network are common paths for malicious users to gain unauthorized access to the network and cardholder data. Unauthorized wireless devices could be hidden within or attached to a computer or other system component. These devices could also be attached directly to a network port, to a network device such as a switch or router, or inserted as a wireless interface card inside a system component. Even if a company has a policy prohibiting the use of wireless technologies, an unauthorized wireless device or network could be installed without the company's knowledge, allowing an attacker to enter the network easily and "invisibly." Detecting and removing such unauthorized access points reduces the duration and likelihood of such devices being leveraged for an attack. *(continued on next page)*
Customized Approach Objective		
Unauthorized wireless access points are identified and addressed periodically.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes The requirement applies even when a policy exists that prohibits the use of wireless technology. Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.		**Good Practice** The size and complexity of an environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment. For example, performing a detailed physical inspection of a single stand-alone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call center, server room or data center), detailed physical inspection can be difficult. In this case, multiple methods may be combined, such as performing physical system inspections in conjunction with the results of a wireless analyzer. **Definitions** This is also referred to as rogue access point detection. **Examples** Methods that may be used include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. NAC and wireless IDS/IPS are examples of automated monitoring tools.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An inventory of authorized wireless access points can help administrators quickly respond when unauthorized wireless access points are detected. This helps to proactively minimize the exposure of CDE to malicious individuals. **Good Practice** If using a wireless scanner, it is equally important to have a defined list of known access points which, while not attached to the company's network, will usually be detected during a scan. These non-company devices are often found in multi-tenant buildings or businesses located near one another. However, it is important to verify that these devices are not connected to the entity's network port or through another network-connected device and given an SSID resembling a nearby business. Scan results should note such devices and how it was determined that these devices could be "ignored." In addition, detection of any unauthorized wireless access points that are determined to be a threat to the CDE should be managed following the entity's incident response plan per Requirement 12.10.1.
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.	**11.2.2** Examine documentation to verify that an inventory of authorized wireless access points is maintained, and a business justification is documented for all authorized wireless access points.	
Customized Approach Objective		
Unauthorized wireless access points are not mistaken for authorized wireless access points.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Identifying and addressing vulnerabilities promptly reduces the likelihood of a vulnerability being exploited and the potential compromise of a system component or cardholder data. Vulnerability scans conducted at least every three months provide this detection and identification. **Good Practice** Vulnerabilities posing the greatest risk to the environment (for example, ranked high or critical per Requirement 6.3.1) should be resolved with the highest priority. Vulnerabilities identified during internal vulnerability scans should be part of a vulnerability management process that includes multiple vulnerability sources, as specified in Requirement 6.3.1. Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved. While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used. *(continued on next page)*
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and all critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	**11.3.1.a** Examine internal scan report results from the last 12 months to verify that internal scans occurred at least once every three months in the most recent 12-month period.	
	11.3.1.b Examine internal scan report results from each scan and rescan run in the last 12 months to verify that all high-risk vulnerabilities and all critical vulnerabilities (defined in PCI DSS Requirement 6.3.1) are resolved.	
	11.3.1.c Examine scan tool configurations and interview personnel to verify that the scan tool is kept up to date with the latest vulnerability information.	
	11.3.1.d Interview responsible personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
Customized Approach Objective		
The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes It is not required to use a QSA or ASV to conduct internal vulnerability scans. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.		**Definitions** A vulnerability scan is a combination of automated tools, techniques, and/or methods run against external and internal devices and servers, designed to expose potential vulnerabilities in applications, operating systems, and network devices that could be found and exploited by malicious individuals.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	**11.3.1.1.a** Examine the entity's targeted risk analysis that defines the risk for addressing all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1.	All vulnerabilities, regardless of criticality, provide a potential avenue of attack and must therefore be addressed periodically, with the vulnerabilities that expose the most risk addressed more quickly to limit the potential window of attack.
Customized Approach Objective	**11.3.1.1.b** Interview responsible personnel and examine internal scan report results or other documentation to verify that all other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis, and that the scan process includes rescans as needed to confirm the vulnerabilities have been addressed.	
Lower ranked vulnerabilities (lower than high-risk or critical) are addressed at a frequency in accordance with the entity's risk.		
Applicability Notes		
The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **11.3.1.2** Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. **Customized Approach Objective** Automated tools used to detect vulnerabilities can detect vulnerabilities local to each system, which are not visible remotely. **Applicability Notes** The authenticated scanning tools can be either host-based or network-based. "Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **11.3.1.2.a** Examine scan tool configurations to verify that authenticated scanning is used for internal scans, with sufficient privileges, for those systems that accept credentials for scanning. **11.3.1.2.b** Examine scan report results and interview personnel to verify that authenticated scans are performed. **11.3.1.2.c** If accounts used for authenticated scanning can be used for interactive login, examine the accounts and interview personnel to verify the accounts are managed following all elements specified in Requirement 8.2.2. **11.3.1.2.d** Examine documentation to verify that systems that are unable to accept credentials for authenticated scanning are defined.	**Purpose** Authenticated scanning provides greater insight into an entity's vulnerability landscape since it can detect vulnerabilities that unauthenticated scans cannot detect. Attackers may leverage vulnerabilities that an entity is unaware of because certain vulnerabilities will only be detected with authenticated scanning. Authenticated scanning can yield significant additional information about an organization's vulnerabilities. **Good Practice** The credentials used for these scans should be considered highly privileged. They should be protected and controlled as such, following PCI DSS Requirements 7 and 8 (except for those requirements for multi-factor authentication and application and system accounts).

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change. **Good Practice** Entities should perform scans after significant changes as part of the change process per Requirement 6.5.2 and before considering the change complete. All system components affected by the change will need to be scanned.
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	**11.3.1.3.a** Examine change control documentation and internal scan reports to verify that system components were scanned after any significant changes. **11.3.1.3.b** Interview personnel and examine internal scan and rescan reports to verify that internal scans were performed after significant changes and that all high-risk vulnerabilities and all critical vulnerabilities (defined in PCI DSS Requirement 6.3.1) were resolved. **11.3.1.3.c** Interview personnel to verify that internal scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
Customized Approach Objective		
The security posture of all system components is verified following significant changes to the network or systems, by using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.		
Applicability Notes		
Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.	**11.3.2.a** Examine ASV scan reports from the last 12 months to verify that external vulnerability scans occurred at least once every three months in the most recent 12-month period.	**Purpose** Attackers routinely look for unpatched or vulnerable externally facing servers, which can be leveraged to launch a directed attack. Organizations must ensure these externally facing devices are regularly scanned for weaknesses and that vulnerabilities are patched or remediated to protect the entity. Because external networks are at greater risk of compromise, external vulnerability scanning must be performed at least once every three months by a PCI SSC Approved Scanning Vendor (ASV). **Good Practice** While scans are required at least once every three months, more frequent scans are recommended depending on the network complexity, frequency of change, and types of devices, software, and operating systems used. Vulnerabilities identified during external vulnerability scans should be part of a vulnerability management process that includes multiple vulnerability sources, as specified in Requirement 6.3.1. Multiple scan reports can be combined to show that all systems were scanned and that all applicable vulnerabilities were resolved as part of the three-month vulnerability scan cycle. However, additional documentation may be required to verify non-remediated vulnerabilities are in the process of being resolved. **Further Information** See the *ASV Program Guide* on the PCI SSC website.
Customized Approach Objective	**11.3.2.b** Examine the ASV scan report from each scan and rescan run in the last 12 months to verify that vulnerabilities are resolved and the *ASV Program Guide* requirements for a passing scan are met.	
This requirement is not eligible for the customized approach.	**11.3.2.c** Examine the ASV scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	
Applicability Notes		
For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Scanning an environment after any significant changes ensures that changes were completed appropriately such that the security of the environment was not compromised because of the change. **Good Practice** Entities should include the need to perform scans after significant changes as part of the change process and before the change is considered complete. All system components affected by the change will need to be scanned.
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	**11.3.2.1.a** Examine change control documentation and external scan reports to verify that system components were scanned after any significant changes.	
	11.3.2.1.b Interview personnel and examine external scan and rescan reports to verify that external scans were performed after significant changes and that vulnerabilities scored 4.0 or higher by the CVSS were resolved.	
Customized Approach Objective	**11.3.2.1.c** Interview personnel to verify that external scans are performed by a qualified internal resource(s) or qualified external third party and that organizational independence of the tester exists.	
The security posture of all system components is verified following significant changes to the network or systems, by using tools designed to detect vulnerabilities operating from outside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Attackers spend a lot of time finding external and internal vulnerabilities to leverage to obtain access to cardholder data and then to exfiltrate that data. As such, entities need to test their networks thoroughly, just as an attacker would do. This testing allows the entity to identify and remediate weakness that might be leveraged to compromise the entity's network and data, and then to take appropriate actions to protect the network and system components from such attacks. **Good Practice** Penetration testing techniques will differ based on an organization's needs and structure and should be suitable for the tested environment—for example, fuzzing, injection, and forgery tests might be appropriate. The type, depth, and complexity of the testing will depend on the specific environment and the needs of the organization. **Definitions** Penetration tests simulate a real-world attack situation intending to identify how far an attacker could penetrate an environment, given differing amounts of information provided to the tester. This allows an entity to better understand its potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that usually includes exploiting identified vulnerabilities. *(continued on next page)*
11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.	**11.4.1** Examine documentation and interview personnel to verify that the penetration-testing methodology defined, documented, and implemented by the entity includes all elements specified in this requirement.	

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker. **Applicability Notes** Testing from inside the network (or "internal penetration testing") means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks. Testing from outside the network (or "external penetration testing") means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.		Scanning for vulnerabilities alone is not a penetration test, nor is a penetration test adequate if the focus is solely on trying to exploit vulnerabilities found in a vulnerability scan. Conducting a vulnerability scan may be one of the first steps, but it is not the only step a penetration tester will perform to plan the testing strategy. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to gain access into an environment. Often the tester will chain several types of exploits together with the goal of breaking through layers of defenses. For example, if the tester finds a way to gain access to an application server, the tester will then use the compromised server as a point to stage a new attack based on the resources to which the server has access. In this way, a tester can simulate the techniques used by an attacker to identify areas of potential weakness in the environment. The testing of security monitoring and detection methods—for example, to confirm the effectiveness of logging and file integrity monitoring mechanisms, should also be considered. *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.4.1 *(continued)*		**Further Information** Refer to the *Information Supplement: Penetration Testing Guidance* for additional guidance. Industry-accepted penetration testing approaches include: *The Open Source Security Testing Methodology and Manual (OSSTMM)* *Open Web Application Security Project (OWASP) penetration testing programs.*
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter. Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the status of many of the controls operating within the CDE. A penetration test is not truly a "test" because the outcome of a penetration test is not something that can be classified as a "pass" or a "fail." The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.	
	11.4.2.b Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	did not know about, and the penetration tester found them before an attacker could. A penetration test that found nothing is typically indicative of shortcomings of the penetration tester, rather than being a positive reflection of the security posture of the entity. **Good Practice** Some considerations when choosing a qualified resource to perform penetration testing include: • Specific penetration testing certifications, which may be an indication of the tester's skill level and competence. • Prior experience conducting penetration testing—for example, the number of years of experience, and the type and scope of prior engagements can help confirm whether the tester's experience is appropriate for the needs of the engagement. **Further Information** Refer to the *Information Supplement: Penetration Testing Guidance* on the PCI SSC website for additional guidance.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV)	**11.4.3.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed according to all elements specified in this requirement.	
	11.4.3.b Interview personnel to verify that the external penetration test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Customized Approach Objective		
External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The results of a penetration test are usually a prioritized list of vulnerabilities discovered by the exercise. Often a tester will have chained a number of vulnerabilities together to compromise a system component. Remediating the vulnerabilities found by a penetration test significantly reduces the probability that the same vulnerabilities will be exploited by a malicious attacker. Using the entity's own vulnerability risk assessment process (see requirement 6.3.1) ensures that the vulnerabilities that pose the highest risk to the entity will be remediated more quickly. **Good Practice** As part of the entity's assessment of risk, entities should consider how likely the vulnerability is to be exploited and whether there are other controls present in the environment to reduce the risk. Any weaknesses that point to PCI DSS requirements not being met should be addressed.
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	**11.4.4** Examine penetration testing results to verify that noted exploitable vulnerabilities and security weaknesses were corrected in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.5.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods in accordance with all elements specified in this requirement. **11.4.5.b** Examine the results from the most recent penetration test to verify the penetration test covers and addresses all elements specified in this requirement. **11.4.5.c** Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Purpose** When an entity uses segmentation controls to isolate the CDE from internal untrusted networks, the security of the CDE is dependent on that segmentation functioning. Many attacks have involved the attacker moving laterally from what an entity deemed an isolated network into the CDE. Using penetration testing tools and techniques to validate that an untrusted network is indeed isolated from the CDE can alert the entity to a failure or misconfiguration of the segmentation controls, which can then be rectified. **Good Practice** Techniques such as host discovery and port scanning can be used to verify out-of-scope segments have no access to the CDE.
Customized Approach Objective		
If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out-of-scope systems.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.6.a** ***Additional testing procedure for service provider assessments only:*** Examine the results from the most recent penetration test to verify that the penetration covers and addressed all elements specified in this requirement. **11.4.6.b** ***Additional testing procedure for service provider assessments only:*** Interview personnel to verify that the test was performed by a qualified internal resource or qualified external third party and that organizational independence of the tester exists (not required to be a QSA or ASV).	**Purpose** Service providers typically have access to greater volumes of cardholder data or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of segmentation controls failing in complex and dynamic networks is greater in service-provider environments. Validating segmentation controls more frequently is likely to discover such failings before they can be exploited by an attacker attempting to pivot laterally from an out-of-scope untrusted network to the CDE. **Good Practice** Although the requirement specifies that this scope validation is carried out at least once every six months and after significant change, this exercise should be performed as frequently as possible to ensure it remains effective at isolating the CDE from other networks.
Customized Approach Objective		
If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
11.4.7 ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	**11.4.7** ***Additional testing procedure for multi-tenant service providers only:*** Examine evidence to verify that multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	Entities need to conduct penetration tests in accordance with PCI DSS to simulate attacker behavior and discover vulnerabilities in their environment. In shared and cloud environments, the multi-tenant service provider may be concerned about the activities of a penetration tester affecting other customers' systems. Multi-tenant service providers cannot forbid penetration testing because this would leave their customers' systems open to exploitation. Therefore, multi-tenant service providers must support customer requests to conduct penetration testing or for penetration testing results.
Customized Approach Objective		
Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a multi-tenant service provider. To meet this requirement, a multi-tenant service provider may either: • Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or • Provide prompt access to each of its customers, so customers can perform their own penetration testing. Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. Refer also to *Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers*. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.5 Network intrusions and unexpected file changes are detected and responded to.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Intrusion-detection and/or intrusion-prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and then send alerts and/or stop the attempt as it happens. Without a proactive approach to detect unauthorized activity, attacks on (or misuse of) computer resources could go unnoticed for long periods of time. The impact of an intrusion into the CDE is, in many ways, a factor of the time that an attacker has in the environment before being detected. **Good Practice** Security alerts generated by these techniques should be continually monitored, so that the attempted or actual intrusions can be stopped, and potential damage limited. **Definitions** Critical locations could include, but are not limited to, network security controls between network segments (for example, between a DMZ and an internal network or between an in-scope and out-of-scope network) and points protecting connections between a less trusted and a more trusted system component.
11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	**11.5.1.a** Examine system configurations and network diagrams to verify that intrusion-detection and/or intrusion-prevention techniques are in place to monitor all traffic: • At the perimeter of the CDE. • At critical points in the CDE.	
	11.5.1.b Examine system configurations and interview responsible personnel to verify intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	
Customized Approach Objective	**11.5.1.c** Examine system configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured to keep all engines, baselines, and signatures up to date.	
Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	**11.5.1.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documentation and configuration settings to verify that methods to detect and alert on/prevent covert malware communication channels are in place and operating.	Detecting covert malware communication attempts (for example, DNS tunneling) can help block the spread of malware laterally inside a network and the exfiltration of data. When deciding where to place this control, entities should consider critical locations in the network, and likely routes for covert channels. When malware establishes a foothold in an infected environment, it often tries to establish a communication channel to a command-and-control (C&C) server. Through the C&C server, the attacker communicates with and controls malware on compromised systems to deliver malicious payloads or instructions, or to initiate data exfiltration. In many cases, the malware will communicate with the C&C server indirectly via botnets, bypassing monitoring, blocking controls, and rendering these methods ineffective to detect the covert channels. *(continued on next page)*
	11.5.1.1.b ***Additional testing procedure for service provider assessments only:*** Examine the entity's incident-response plan (Requirement 12.10.1) to verify it requires and defines a response in the event that covert malware communication channels are detected.	
Customized Approach Objective	**11.5.1.1.c** ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and observe processes to verify that personnel maintain knowledge of covert malware communication and control techniques and are knowledgeable about how to respond when malware is suspected.	
Mechanisms are in place to detect and alert/prevent covert communications with command-and-control systems. Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that such communications are blocked. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Good Practice** Methods that can help detect and address malware communications channels include real-time endpoint scanning, egress traffic filtering, an ”allow” listing, data loss prevention tools, and network security monitoring tools such as IDS/IPS. Additionally, DNS queries and responses are a key data source used by network defenders in support of incident response as well as intrusion discovery. When these transactions are collected for processing and analytics, they can enable a number of valuable security analytic scenarios. It is important that organizations maintain up-to-date knowledge of malware modes of operation, as mitigating these can help detect and limit the impact of malware in the environment.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	**11.5.2.a** Examine system settings, monitored files, and results from monitoring activities to verify the use of a change-detection mechanism.	Changes to critical system, configuration, or content files can be an indicator an attacker has accessed an organization's system. Such changes can allow an attacker to take additional malicious actions, access cardholder data, and/or conduct activities without detection or record. A change detection mechanism will detect and evaluate such changes to critical files and generate alerts that can be responded to following defined processes so that personnel can take appropriate actions. *(continued on next page)*
Customized Approach Objective	**11.5.2.b** Examine settings for the change-detection mechanism to verify it is configured in accordance with all elements specified in this requirement.	
Critical files cannot be modified by unauthorized personnel without an alert being generated. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).		If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing. **Good Practice** Examples of the types of files that should be monitored include, but are not limited to: • System executables. • Application executables. • Configuration and parameter files. • Centrally stored, historical, or archived audit logs. • Additional critical files determined by entity (for example, through risk assessment or other means). **Examples** Change-detection solutions such as file integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
11.6 Unauthorized changes on payment pages are detected and responded to.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Many web pages now rely on assembling objects, including active content (primarily JavaScript), from multiple internet locations. Additionally, the content of many web pages is defined using content management and tag management systems that may not be possible to monitor using traditional change detection mechanisms. Therefore, the only place to detect changes or indicators of malicious activity is in the consumer browser as the page is constructed and all JavaScript interpreted. By comparing the current version of the HTTP header and the active content of payment pages as received by the consumer browser with prior or known versions, it is possible to detect unauthorized changes that may indicate a skimming attack, or an attempt to disable a control designed to protect against, or to detect, skimming attacks. Additionally, by looking for known indicators of compromise and script elements or behavior typical of skimmers, suspicious alerts can be raised. *(continued on next page)*
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP headers and payment pages. • The mechanism functions are performed as follows: – At least weekly **OR** – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	**11.6.1.a** Examine system settings, monitored payment pages, and results from monitoring activities to verify the use of a change- and tamper-detection mechanism. **11.6.1.b** Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement. **11.6.1.c** If the mechanism functions are performed at an entity-defined frequency, examine the entity's targeted risk analysis for determining the frequency to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1. **11.6.1.d** Examine configuration settings and interview personnel to verify the mechanism functions are performed either: • At least weekly **OR** • At the frequency defined in the entity's targeted risk analysis performed for this requirement.	
Customized Approach Objective		
E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes This requirement also applies to entities with a webpage(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes.) This requirement does not apply to an entity for scripts in a TPSP's/payment processor's embedded payment page/form (for example, one or more iframes), where the entity includes a TPSP's/payment processor's payment page/form on its webpage. Scripts in the TPSP's/payment processor's embedded payment page/form are the responsibility of the TPSP/payment processor to manage in accordance with this requirement. The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the Guidance column to prevent and detect unexpected script activities. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Good Practice** Where an entity includes a TPSP's/payment processor's embedded payment page/form on its webpage, the entity should expect the TPSP/payment processor to provide evidence that the TPSP/payment processor is meeting this requirement, in accordance with the TPSP's/payment processor's PCI DSS assessment and Requirement 12.9. **Examples** Mechanisms that detect and report on changes to the headers and content of the payment page could include, but are not limited to, a combination of the following techniques: • Violations of the Content Security Policy (CSP) can be reported to the entity using the *report-to* or *report-uri* CSP directives. • Changes to the CSP itself can indicate tampering. • External monitoring by systems that request and analyze the received web pages (also known as synthetic user monitoring) can detect changes to JavaScript in payment pages and alert personnel. • Embedding tamper-resistant, tamper-detection script in the payment page can alert and block when malicious script behavior is detected. • Reverse proxies and Content Delivery Networks can detect changes in scripts and alert personnel. The above list of mechanisms is not exhaustive, and the use of any one mechanism is not necessarily a full detection and reporting mechanism. Often, these mechanisms are subscription or cloud-based, but can also be based on custom and bespoke solutions.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Sections

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

Overview

The organization's overall information security policy sets the tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of cardholder data and/or sensitive authentication data.

Refer to *Appendix G* for definitions of PCI DSS terms.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	**12.1.1** Examine the information security policy and interview personnel to verify that the overall information security policy is managed in accordance with all elements specified in this requirement.	An organization's overall information security policy ties to and governs all other policies and procedures that define protection of cardholder data. The information security policy communicates management's intent and objectives regarding the protection of its most valuable assets, including cardholder data. Without an information security policy, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its legal, regulatory, and contractual obligations, nor being able to adequately protect its assets in a consistent manner. To ensure the policy is implemented, it is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization's information security policy and their responsibilities for protecting information assets. *(continued on next page)*
Customized Approach Objective		
The strategic objectives and principles of information security are defined, adopted, and known to all personnel.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.1.1 *(continued)*		**Good Practice** The security policy for the organization identifies the purpose, scope, accountability, and information that clearly defines the organization's position regarding information security. The overall information security policy differs from individual security policies that address specific technology or security disciplines. This policy sets forth the directives for the entire organization whereas individual security policies align and support the overall security policy and communicate specific objectives for technology or security disciplines. It is important that all relevant personnel within the organization, as well as relevant third parties, vendors, and business partners are aware of the organization's information security policy and their responsibilities for protecting information assets. **Definitions** "Relevant" for this requirement means that the information security policy is disseminated to those with roles applicable to some or all the topics in the policy, either within the company or because of services/functions performed by a vendor or third party.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	**12.1.2** Examine the information security policy and interview responsible personnel to verify the policy is managed in accordance with all elements specified in this requirement.	Security threats and associated protection methods evolve rapidly. Without updating the information security policy to reflect relevant changes, new measures to defend against these threats may not be addressed.
Customized Approach Objective		
The information security policy continues to reflect the organization's strategic objectives and principles.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	**12.1.3.a** Examine the information security policy to verify that they clearly define information security roles and responsibilities for all personnel.	Without clearly defined security roles and responsibilities assigned, there could be misuse of the organization's information assets or inconsistent interaction with information security personnel, leading to insecure implementation of technologies or use of outdated or insecure technologies.
	12.1.3.b Interview personnel in various roles to verify they understand their information security responsibilities.	
	12.1.3.c Examine documented evidence to verify personnel acknowledge their information security responsibilities.	
Customized Approach Objective		
Personnel understand their role in protecting the entity's cardholder data.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** To ensure someone with sufficient authority and responsibility is actively managing and championing the organization's information security program, accountability and responsibility for information security needs to be assigned at the executive level within an organization. **Good Practice** These executive management positions are often at the most senior level of management and are part of the chief executive level or C-level, typically reporting to the Chief Executive Officer or the Board of Directors. Information security knowledge for this executive management role can be indicated by work experience, education, and/or relevant professional certifications. The expectation is that this individual can provide assurance about the implementation of an effective security program and ensure the right technical experts are employed. Entities should also consider transition and/or succession plans for these key personnel to avoid potential gaps in critical security activities.
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management. .	**12.1.4** Examine the information security policy to verify that information security is formally assigned to a Chief Information Security Officer or other information security-knowledgeable member of executive management.	
Customized Approach Objective		
A designated member of executive management is responsible for information security.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.2 Acceptable use policies for end-user technologies are defined and implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	**12.2.1** Examine the acceptable use policies for end-user technologies and interview responsible personnel to verify processes are documented and implemented in accordance with all elements specified in this requirement.	End-user technologies are a significant investment and may pose significant risk to an organization if not managed properly. Acceptable use policies outline the expected behavior from personnel when using the organization's information technology and reflect the organization's risk tolerance These policies instruct personnel on what they can and cannot do with company equipment and instruct personnel on correct and incorrect uses of company Internet and email resources. Such policies can legally protect an organization and allow it to act when the policies are violated. **Good Practice** It is important that usage policies are supported by technical controls to manage the enforcement of the policies. Structuring polices as simple "do" and "do not" requirements that are linked to a purpose can help remove ambiguity and provide personnel with the context for the requirement.
Customized Approach Objective		
The use of end-user technologies is defined and managed to ensure authorized usage.		
Applicability Notes		
Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, email usage, and Internet usage.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	**12.3.1** Examine documented policies and procedures to verify a process is defined for performing targeted risk analyses for each PCI DSS requirement that specifies completion of a targeted risk analysis, and that the process includes all elements specified in this requirement.	Some PCI DSS requirements allow an entity to define how frequently an activity is performed based on the risk to the entity's environment. Performing this risk analysis according to a methodology ensures validity and consistency with policies and procedures. This targeted risk analysis (as opposed to a traditional enterprise-wide risk assessment) focuses on those PCI DSS requirements that allow an entity flexibility about how frequently an entity performs a given control. For this risk analysis, the entity carefully evaluates each PCI DSS requirement that provides this flexibility and determines the frequency that supports adequate security for the entity, and the level of risk the entity is willing to accept. The risk analysis identifies the specific assets, such as the system components and data—for example, log files, or credentials—that the requirement is intended to protect, as well as the threat(s) or outcomes that the requirement is protecting the assets from—for example, malware, an undetected intruder, or misuse of credentials. Examples of factors that could contribute to likelihood or impact include any that could increase the vulnerability of an asset to a threat—for example, exposure to untrusted networks, complexity of environment, or high staff turnover—as well as the criticality of the system components, or volume and sensitivity of the data, being protected. *(continued on next page)*
Customized Approach Objective		
Up to date knowledge and assessment of risks to the CDE are maintained.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.3.1 *(continued)*		Reviewing the results of these targeted risk analyses at least once every 12 months and upon changes that could impact the risk to the environment allows the organization to ensure the risk analysis results remain current with organizational changes and evolving threats, trends, and technologies, and that the selected frequencies still adequately address the entity's risk. **Good Practice** An enterprise-wide risk assessment, which is a point-in-time activity that enables entities to identify threats and associated vulnerabilities, is recommended, but is not required, for entities to determine and understand broader and emerging threats with the potential to negatively impact its business. This enterprise-wide risk assessment could be established as part of an overarching risk management program that is used as an input to the annual review of an organization's overall information security policy (see Requirement 12.1.1). Examples of risk-assessment methodologies for enterprise-wide risk assessments include, but are not limited to, ISO *27005* and NIST *SP 800-30*. **Further Information** Refer to the following documents on the PCI SSC website: • *Information Supplement: TRA Guidance* • *Sample Template: TRA for Activity Frequency*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A risk analysis following a repeatable and robust methodology enables an entity to meet the customized approach objective. **Definitions** The customized approach to meeting a PCI DSS requirement allows entities to define the controls used to meet a given requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. These controls are expected to at least meet or exceed the security provided by the defined requirement and require extensive documentation by the entity using the customized approach. **Further Information** See *Appendix D: Customized Approach* for instructions on how to document the required evidence for the customized approach. See *PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website for templates that entities may use to document their customized controls. Note that while use of the templates is optional, the information specified within each template must be documented and provided to each entity's assessor.
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.	**12.3.2** Examine the documented targeted risk-analysis for each PCI DSS requirement that the entity meets with the customized approach to verify that documentation for each requirement exists and is in accordance with all elements specified in this requirement.	
Customized Approach Objective This requirement is part of the customized approach and must be met for those using the customized approach.		
Applicability Notes This requirement only applies to entities using a Customized Approach.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, proactive plans will help the entity to upgrade before the deprecation is impactful to operations. **Definitions** "Cryptographic agility" refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • Documentation of a plan, to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic cipher suites and protocols used to meet PCI DSS requirements, including, but not limited to, those used to render PAN unreadable in storage and transmission, to protect passwords, and as part of authenticating access. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies to ensure that they can prepare for, and manage, vulnerabilities in hardware and software that will not be remediated by the vendor or developer. **Good Practice** Organizations should review firmware versions to ensure they remain current and supported by the vendors. Organizations also need to be aware of changes made by technology vendors to their products or processes to understand how such changes may impact the organization's use of the technology. Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies, and ensure controls that rely on those technologies remain effective. These reviews include, but are not limited to, reviewing technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	**12.3.4** Examine documentation for the review of hardware and software technologies in use and interview personnel to verify that the review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.4 PCI DSS compliance is managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	**12.4.1** ***Additional testing procedure for service provider assessments only:*** Examine documentation to verify that executive management has established responsibility for the protection of cardholder data and a PCI DSS compliance program in accordance with all elements specified in this requirement.	Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities.
Customized Approach Objective		
Executives are responsible and accountable for security of cardholder data.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. This requirement is distinct from other requirements that specify a task to be performed. The objective of these reviews is not to reperform other PCI DSS requirements, but to confirm that security activities are being performed on an ongoing basis. **Good Practice** These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment. **Examples** Looking at Requirement 1.2.7 as one example, Requirement 12.4.2 is met by confirming, at least once every three months, that reviews of configurations of network security controls have occurred at the required frequency. On the other hand, Requirement 1.2.7 is met by reviewing those configurations as specified in the requirement.
12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.	**12.4.2.a** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify that processes are defined for conducting reviews to confirm that personnel are performing their tasks in accordance with all security policies and all operational procedures, including but not limited to the tasks specified in this requirement.	
	12.4.2.b ***Additional testing procedure for service provider assessments only:*** Interview responsible personnel and examine records of reviews to verify that reviews are performed: • At least once every three months. • By personnel other than those responsible for performing the given task.	
Customized Approach Objective		
The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.4.2.1 ***Additional requirement for service providers only:*** Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	**12.4.2.1** ***Additional testing procedure for service provider assessments only:*** Examine documentation from the reviews conducted in accordance with PCI DSS Requirement 12.4.2 to verify the documentation includes all elements specified in this requirement.	The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment.
Customized Approach Objective		
Findings from operational effectiveness reviews are evaluated by management; appropriate remediation activities are implemented.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.5 PCI DSS scope is documented and validated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining a current list of all system components will enable an organization to define the scope of its environment and implement PCI DSS requirements accurately and efficiently. Without an inventory, some system components could be overlooked and be inadvertently excluded from the organization's configuration standards. **Good Practice** If an entity keeps an inventory of all assets, those system components in scope for PCI DSS should be clearly identifiable among the other assets. Inventories should include containers or images that may be instantiated. Assigning an owner to the inventory helps to ensure the inventory stays current. **Examples** Methods to maintain an inventory include as a database, as a series of files, or in an inventory-management tool.
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	**12.5.1.a** Examine the inventory to verify it includes all in-scope system components and a description of function/use for each.	
	12.5.1.b Interview personnel to verify the inventory is kept current.	
Customized Approach Objective		
All system components in scope for PCI DSS are identified and known.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	**12.5.2.a** Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every 12 months. • After significant changes to the in-scope environment. **12.5.2.b** Examine documented results of scope reviews performed by the entity to verify that PCI DSS scoping confirmation activity includes all elements specified in this requirement.	**Purpose** Frequent validation of PCI DSS scope helps to ensure PCI DSS scope remains up to date and aligned with changing business objectives, and therefore that security controls are protecting all appropriate system components. **Good Practice** Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information: • Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period, • Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization), • How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization), • How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.). *(continued on next page)*

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Customized Approach Objective PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures. **Applicability Notes** This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.		In addition to internal systems and networks, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls can be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE. A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured. **Further Information** For additional guidance, refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	**12.5.2.1.a** ***Additional testing procedure for service provider assessments only:*** Examine documented results of scope reviews and interview personnel to verify that reviews per Requirement 12.5.2 are performed: • At least once every six months, and • After significant changes	Service providers typically have access to greater volumes of cardholder data than do merchants, or can provide an entry point that can be exploited to then compromise multiple other entities. Service providers also typically have larger and more complex networks that are subject to more frequent change. The probability of overlooked changes to scope in complex and dynamic networks is greater in service-providers environments. Validating PCI DSS scope more frequently is likely to discover such overlooked changes before they can be exploited by an attacker.
Customized Approach Objective	**12.5.2.1.b** ***Additional testing procedure for service provider assessments only:*** Examine documented results of scope reviews to verify that scoping validation includes all elements specified in Requirement 12.5.2.	
The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to an organization's structure and management to ensure controls are in place and active. **Examples** Changes to organizational structure include, but are not limited to, company mergers or acquisitions, and significant changes or reassignments of personnel with responsibility for security controls.
12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	**12.5.3.a** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify that processes are defined such that a significant change to organizational structure results in documented review of the impact to PCI DSS scope and applicability of controls.	
Customized Approach Objective	**12.5.3.b** ***Additional testing procedure for service provider assessments only:*** Examine documentation (for example, meeting minutes) and interview responsible personnel to verify that significant changes to organizational structure resulted in documented reviews that included all elements specified in this requirement, with results communicated to executive management.	
PCI DSS scope is confirmed after significant organizational change.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.6 Security awareness education is an ongoing activity.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	**12.6.1** Examine the security awareness program to verify it provides awareness to all personnel about the entity's information security policy and procedures, and personnel's role in protecting the cardholder data.	If personnel are not educated about their company's information security policies and procedures and their own security responsibilities, security safeguards and processes that have been implemented may become ineffective through unintentional errors or intentional actions.
Customized Approach Objective		
Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's cardholder data and/or sensitive authentication data, or the information provided to personnel about their role in protecting cardholder data.	**12.6.2** Examine security awareness program content, evidence of reviews, and interview personnel to verify that the security awareness program is in accordance with all elements specified in this requirement.	The threat environment and an entity's defenses are not static. As such, the security awareness program materials must be updated as frequently as needed to ensure that the education received by personnel is up to date and represents the current threat environment.
Customized Approach Objective		
The content of security awareness material is reviewed and updated periodically.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	**12.6.3.a** Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months. **12.6.3.b** Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel.	**Purpose** Training of personnel ensures they receive the information about the importance of information security and that they understand their role in protecting the organization. Requiring an acknowledgment by personnel helps ensure that they have read and understood the security policies and procedures, and that they have made and will continue to make a commitment to comply with these policies. **Good Practice** Entities may incorporate new-hire training as part of the Human Resources onboarding process. Training should outline the security-related “dos” and “don’ts.” Periodic refresher training reinforces key security processes and procedures that may be forgotten or bypassed. Entities should consider requiring security awareness training anytime personnel transfer into roles where they can impact the security of cardholder data and/or sensitive authentication data from roles where they did not have this impact. Methods and training content can vary, depending on personnel roles. **Examples** Different methods that can be used to provide security awareness and education include posters, letters, web-based training, in-person training, team meetings, and incentives. Personnel acknowledgments may be recorded in writing or electronically.
	12.6.3.c Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data.	
Customized Approach Objective	**12.6.3.d** Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.	
Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Educating personnel on how to detect, react to, and report potential phishing and related attacks and social engineering attempts is essential to minimizing the probability of successful attacks. **Good Practice** An effective security awareness program should include examples of phishing emails and periodic testing to determine the prevalence of personnel reporting such attacks. Training material an entity can consider for this topic include: • How to identify phishing and other social engineering attacks. • How to react to suspected phishing and social engineering. • Where and how to report suspected phishing and social engineering activity. An emphasis on reporting allows the organization to reward positive behavior, to optimize technical defenses (see Requirement 5.4.1), and to take immediate action to remove similar phishing emails that evaded technical defenses from recipient inboxes.
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to: • Phishing and related attacks. • Social engineering.	**12.6.3.1** Examine security awareness training content to verify it includes all elements specified in this requirement.	
Customized Approach Objective		
Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.		
Applicability Notes		
See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	**12.6.3.2** Examine security awareness training content to verify it includes awareness about acceptable use of end-user technologies in accordance with Requirement 12.2.1.	By including the key points of the acceptable use policy in regular training and the related context, personnel will understand their responsibilities and how these impact the security of an organization's systems.
Customized Approach Objective		
Personnel are knowledgeable about their responsibility for the security and operation of end-user technologies and are able to access assistance and guidance when required.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.7 Personnel are screened to reduce risks from insider threats.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Performing thorough screening prior to hiring potential personnel who are expected to be given access to the CDE provides entities with the information necessary to make informed risk decisions regarding personnel they hire that will have access to the CDE. Other benefits of screening potential personnel include helping to ensure workplace safety and confirming information provided by prospective employees on their resumes. **Good Practice** Entities should consider screening for existing personnel anytime they transfer into roles where they have access to the CDE from roles where they did not have this access. To be effective, the level of screening should be appropriate for the position. For example, positions requiring greater responsibility or that have administrative access to critical data or systems may warrant more detailed or more frequent screening than positions with less responsibility and access. **Examples** Screening options can include, as appropriate for the entity's region, previous employment history, review of public information/social media resources, criminal record, credit history, and reference checks.
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	**12.7.1** Interview responsible Human Resource department management to verify that screening is conducted, within the constraints of local laws, prior to hiring potential personnel who will have access to the CDE.	
Customized Approach Objective		
The risk related to allowing new members of staff access to the CDE is understood and managed.		
Applicability Notes		
For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface. **Examples** Different types of TPSPs include those that: • Store, process, or transmit account data on the entity's behalf (such as payment gateways, payment processors, payment service providers (PSPs), and off-site storage providers). • Manage system components included in the entity's PCI DSS assessment (such as providers of network security control services, anti-malware services, and security incident and event management (SIEM); contact and call centers; web-hosting companies; and IaaS, PaaS, SaaS, and FaaS cloud providers). • Could impact the security of the entity's cardholder data and/or sensitive authentication data (such as vendors providing support via remote access, and bespoke software developers).
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	**12.8.1.a** Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	
	12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	
Customized Approach Objective		
Records are maintained of TPSPs and the services provided.		
Applicability Notes		
The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The written acknowledgment from a TPSP demonstrates its commitment to maintaining proper security of account data that it obtains from its customers and that the TPSP is fully aware of the assets that could be affected during the provisioning of the TPSP's service. The extent to which a specific TPSP is responsible for the security of account data will depend on the service provided and the responsibilities agreed between the provider and assessed entity (the customer). In conjunction with Requirement 12.9.1, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	**12.8.2.a** Examine policies and procedures to verify that processes are defined to maintain written agreements with all TPSPs in accordance with all elements specified in this requirement.	
	12.8.2.b Examine written agreements with TPSPs to verify they are maintained in accordance with all elements as specified in this requirement.	
Customized Approach Objective		
Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements (is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.		**Good Practice** The entity may also want to consider including in their written agreement with a TPSP that the TPSP will support the entity's request for information per Requirement 12.9.2. Entities will also want to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service. It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and what types of written agreements the primary TPSP has in place with the secondary TPSPs. Entities can consider including coverage in their written agreement for any "nested" TPSPs a primary TPSP may use. **Further Information** Refer to the *Information Supplement: Third-Party Security Assurance* for further guidance.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="4">Purpose
A thorough process for engaging TPSPs, including details for selection and vetting prior to engagement, helps ensure that a TPSP is thoroughly vetted internally by an entity prior to establishing a formal relationship and that the risk to cardholder data associated with the engagement of the TPSP is understood.
Good Practice
Specific due-diligence processes and goals will vary for each organization. Elements that should be considered include the provider’s reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the TPSP validates their PCI DSS compliance and what evidence they provide.</td></tr>
<tr><td rowspan="2">12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.</td><td>12.8.3.a Examine policies and procedures to verify that processes are defined for engaging TPSPs, including proper due diligence prior to engagement.</td></tr>
<tr><td rowspan="2">12.8.3.b Examine evidence and interview responsible personnel to verify the process for engaging TPSPs includes proper due diligence prior to engagement.</td></tr>
<tr><td>Customized Approach Objective</td></tr>
<tr><td>The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.</td><td></td></tr>
</table>

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Knowing the PCI DSS compliance status of all engaged TPSPs provides assurance and awareness about whether they comply with the requirements applicable to the services they offer to the organization. **Good Practice** If the TPSP offers a variety of services, the compliance status the entity monitors should be specific to those services delivered to the entity and those services in scope for the entity's PCI DSS assessment. *(continued on next page)*
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	**12.8.4.a** Examine policies and procedures to verify that processes are defined to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	
	12.8.4.b Examine documentation and interview responsible personnel to verify that the PCI DSS compliance status of each TPSP is monitored at least once every 12 months.	
Customized Approach Objective		
The PCI DSS compliance status of TPSPs is verified periodically.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.		If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, it may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met. **Further Information** For more information about third-party service providers, refer to: • PCI DSS section: Use of Third-Party Service Providers. • *Information Supplement: Third-Party Security Assurance*.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important that the entity understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the entity, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. Without this shared understanding, it is inevitable that the entity and the TPSP will assume a given PCI DSS sub-requirement is the responsibility of the other party, and therefore that sub-requirement may not be addressed at all. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the entity and TPSP. **Good Practice** Entities can document these responsibilities via a matrix that identifies all applicable PCI DSS requirements and indicates for each requirement whether the entity or TPSP is responsible for meeting that requirement or whether it is a shared responsibility. This type of document is often referred to as a *responsibility matrix*. *(continued on next page)*
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	**12.8.5.a** Examine policies and procedures to verify that processes are defined to maintain information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both the TPSP and the entity.	
	12.8.5.b Examine documentation and interview personnel to verify the entity maintains information about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between both entities.	
Customized Approach Objective		
Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.8.5 *(continued)*		It is also important for entities to understand whether any TPSPs have "nested" relationships with other TPSPs, meaning the primary TPSP contracts with another TPSP(s) for the purposes of providing a service. It is important to understand whether the primary TPSP is relying on the secondary TPSP(s) to achieve overall compliance of a service, and how the primary TPSP is monitoring performance of the service and the PCI DSS compliance status of the secondary TPSP(s). Note that it is the responsibility of the primary TPSP to manage and monitor any secondary TPSPs. **Further Information** Refer to *Information Supplement: Third-Party Security Assurance* for a sample responsibility matrix template.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.9.1 ***Additional requirement for service providers only:*** TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.	**12.9.1** ***Additional testing procedure for service provider assessments only:*** Examine TPSP policies, procedures, and templates used for written agreements to verify processes are defined for the TPSP to provide written acknowledgments to customers in accordance with all elements specified in this requirement.	In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between TPSPs and their customers about their applicable PCI DSS responsibilities. The acknowledgment from the TPSP evidences the TPSP's commitment to maintaining proper security of the account data that it obtains from its customers. The TPSP's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to its customers. The method by which the TPSP provides written acknowledgment should be agreed between the provider and its customers.
Customized Approach Objective		
TPSPs formally acknowledge their security responsibilities to their customers. *(continued on next page)*		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider. The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements is not the same as a written agreement specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations. **Good Practice** If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, they may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met. TPSPs should provide sufficient evidence to their customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. *(continued on next page)*
12.9.2 ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data or sensitive authentication data.	**12.9.2** ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.	
Customized Approach Objective		
TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.9.2 *(continued)*		TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the customer and TPSP. It is important that the customer understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the customer, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. An example of a way to document these responsibilities is via a matrix that identifies all applicable PCI DSS requirements and indicates whether the customer or TPSP is responsible for meeting that requirement or whether it is a shared responsibility. **Further Information** For further guidance, refer to: • PCI DSS section: *Use of Third-Party Service Providers*. • *Information Supplement: Third-Party Security Assurance* (includes a sample responsibility matrix template).

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without a comprehensive incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as risk of financial and/or reputational loss and legal liabilities. **Good Practice** The incident response plan should be thorough and contain all the key elements for stakeholders (for example, legal, communications) to allow the entity to respond effectively in the event of a breach that could impact account data. It is important to keep the plan up to date with current contact information of all individuals designated as having a role in incident response. Other relevant parties for notifications may include customers, financial institutions (acquirers and issuers), and business partners. Entities should consider how to address all compromises of data within the CDE in their incident response plans, including compromises to account data, wireless encryption keys, encryption keys used for transmission and storage or account data or cardholder data, etc. *(continued on next page)*
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	**12.10.1.a** Examine the incident response plan to verify that the plan exists and includes at least the elements specified in this requirement. **12.10.1.b** Interview personnel and examine documentation from previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.	
Customized Approach Objective		
A comprehensive incident response plan that meets card brand expectations is maintained.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
12.10.1 *(continued)*		**Examples** Legal requirements for reporting compromises include those in most US states, the EU General Data Protection Regulation (GDPR), and the Personal Data Protection Act (Singapore). **Further Information** For more information, refer to the *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Proper testing of the security incident response plan can identify broken business processes and ensure key steps are not missed, which could result in increased exposure during an incident. Periodic testing of the plan ensures that the processes remain viable, as well as ensuring that all relevant personnel in the organization are familiar with the plan. **Good Practice** The test of the incident response plan can include simulated incidents and the corresponding responses in the form of a "table-top exercise" that includes participation by relevant personnel. A review of the incident and the quality of the response can provide entities with the assurance that all required elements are included in the plan.
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	**12.10.2** Interview personnel and review documentation to verify that, at least once every 12 months, the security incident response plan is: • Reviewed and updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	
Customized Approach Objective		
The incident response plan is kept current and tested periodically.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An incident could occur at any time, therefore if a person who is trained in incident response and familiar with the entity's plan is available when an incident is detected, the entity's ability to correctly respond to the incident is increased. **Good Practice** Often, specific personnel are designated to be part of a security incident response team, with the team having overall responsibility for responding to incidents (perhaps on a rotating schedule basis) and managing those incidents in accordance with the plan. The incident response team can consist of core members who are permanently assigned or "on-demand" personnel who may be called up as necessary, depending on their expertise and the specifics of the incident. Having available resources to respond quickly to incidents minimizes disruption to the organization. Examples of types of activity the team or individuals should respond to include any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	**12.10.3** Examine documentation and interview responsible personnel occupying designated roles to verify that specific personnel are designated to be available on a 24/7 basis to respond to security incidents.	
Customized Approach Objective		
Incidents are responded to immediately where appropriate.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **12.10.4** Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. **Customized Approach Objective** Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.	**Defined Approach Testing Procedures** **12.10.4** Examine training documentation and interview incident response personnel to verify that personnel are appropriately and periodically trained on their incident response responsibilities.	**Purpose** Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation. **Good Practice** It is important that all personnel involved in incident response are trained and knowledgeable about managing evidence for forensics and investigations.
Defined Approach Requirements **12.10.4.1** The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **Customized Approach Objective** Incident response personnel are trained at a frequency that addresses the entity's risk. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **12.10.4.1.a** Examine the entity's targeted risk analysis for the frequency of training for incident response personnel to verify the risk analysis was performed in accordance with all elements specified in Requirement 12.3.1. **12.10.4.1.b** Examine documented results of periodic training of incident response personnel and interview personnel to verify training is performed at the frequency defined in the entity's targeted risk analysis performed for this requirement.	**Purpose** Each entity's environment and incident response plan are different, and the approach will depend on a number of factors, including the size and complexity of the entity, the degree of change in the environment, the size of the incident response team, and the turnover in personnel. Performing a risk analysis will allow the entity to determine the optimum frequency for training personnel with incident response responsibilities.

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points.	**12.10.5** Examine documentation and observe incident response processes to verify that monitoring and responding to alerts from security monitoring systems are covered in the security incident response plan, including but not limited to the systems specified in this requirement.	Responding to alerts generated by security monitoring systems that are explicitly designed to focus on potential risk to data is critical to prevent a breach and therefore, this must be included in the incident-response processes.
Customized Approach Objective		
Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.		
Applicability Notes		
The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Incorporating lessons learned into the incident response plan after an incident occurs and in-step with industry developments, helps keep the plan current and able to react to emerging threats and security trends. **Good Practice** The lessons-learned exercise should include all levels of personnel. Although it is often included as part of the review of the entire incident, it should focus on how the entity's response to the incident could be improved. It is important to not just consider elements of the response that did not have the planned outcomes but also to understand what worked well and whether lessons from those elements that worked well can be applied to areas of the plan that did not. Another way to optimize an entity's incident response plan is to understand the attacks made against other organizations and use that information to fine-tune the entity's detection, containment, mitigation, or recovery procedures.
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	**12.10.6.a** Examine policies and procedures to verify that processes are defined to modify and evolve the security incident response plan according to lessons learned and to incorporate industry developments.	
	12.10.6.b Examine the security incident response plan and interview responsible personnel to verify that the incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	
Customized Approach Objective		
The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having documented incident response procedures that are followed in the event that stored PAN is found anywhere it is not expected to be, helps to identify the necessary remediation actions and prevent future leaks. **Good Practice** If PAN was found outside the CDE, analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE. Entities should consider whether there are contributory factors, such as business processes, user behavior, improper system configurations, etc. that caused the PAN to be stored in an unexpected location. If such contributory factors are present, they should be addressed per this Requirement to prevent recurrence.
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	**12.10.7.a** Examine documented incident response procedures to verify that procedures for responding to the detection of stored PAN anywhere it is not expected to exist, ready to be initiated, and include all elements specified in this requirement.	
	12.10.7.b Interview personnel and examine records of response actions to verify that incident response procedures are performed upon detection of stored PAN anywhere it is not expected.	
Customized Approach Objective		
Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

©2006 - 2024 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A Additional PCI DSS Requirements

This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include:

- Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers
- Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/early TLS for Card-Present POS POI Terminal Connections
- Appendix A3: Designated Entities Supplemental Validation (DESV)

Guidance and applicability information is provided in each section.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

Sections
A1.1 Multi-tenant service providers protect and separate all customer environments and data.
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.

Overview
All service providers are responsible for meeting PCI DSS requirements for their own environments as applicable to the services offered to their customers. In addition, multi-tenant service providers must meet the requirements in this Appendix.
Multi-tenant service providers are a type of third-party service provider that offers various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or "shopping cart" services, web-based hosting services, payment applications, various cloud applications and services, and payment gateway and processor services offered in a shared environment.
Service providers that provide only shared data center services (often called co-location or "co-lo" providers), where equipment, space, and bandwidth are available on a rental basis, are not considered multi-tenant service providers for purposes of this Appendix.
***Note**: Even though a multi-tenant service provider may meet these requirements, each customer is still responsible to comply with the PCI DSS requirements that are applicable to its environment and validate compliance as applicable. Often, there are PCI DSS requirements for which responsibility is shared between the provider and the customer (for perhaps different aspects of the environment). Requirements 12.8 and 12.9 delineate requirements specific to the relationships between all third-party service providers (TPSPs) and their customers, and the responsibilities of both. This includes defining the specific services the customer is receiving, along with which PCI DSS requirements are the responsibility of the customer to meet, which are the responsibility of the TPSP, and which requirements are shared between both customer and the TPSP.*

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A1.1 Multi-tenant service providers protect and separate all customer environments and data.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization.	**A1.1.1** Examine documentation and system and network configurations and interview personnel to verify that logical separation is implemented in accordance with all elements specified in this requirement.	Without controls between the provider's environment and the customer's environment, a malicious actor within the provider's environment could compromise the customer's environment, and similarly, a malicious actor in a customer environment could compromise the provider and potentially other of the provider's customers. Multi-tenant environments should be isolated from each other and from the provider's infrastructure such that they can be separately managed entities with no connectivity between them. **Good Practice** Providers should ensure strong separation between the environments that are designed for customer access, for example, configuration and billing portals, and the provider's private environment that should only be accessed by authorized provider personnel. Service provider access to customer environments is performed in accordance with requirement 8.2.3. **Further Information** Refer to the *Information Supplement: PCI SSC Cloud Computing Guidelines* for further guidance on cloud environments.
Customized Approach Objective		
Customers cannot access the provider's environment. The provider cannot access its customers' environments without authorization.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="3">Purpose
It is important that a multi-tenant service provider define controls so that each customer can only access their own environment and CDE to prevent unauthorized access from one customer's environment to another.
Examples
In a cloud-based infrastructure, such as an infrastructure as a service (IaaS) offering, the customers' CDE may include virtual network devices and virtual servers that are configured and managed by the customers, including operating systems, files, memory, etc.</td></tr>
<tr><td>A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.</td><td>A1.1.2.a Examine documentation to verify controls are defined such that each customer only has permission to access its own cardholder data and CDE.</td></tr>
<tr><td>Customized Approach Objective
Customers cannot access other customers' environments.</td><td>A1.1.2.b Examine system configurations to verify that customers have privileges established to only access their own account data and CDE.</td></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="3">Purpose
To prevent any inadvertent or intentional impact to other customers' environments or account data, it is important that each customer can access only resources allocated to that customer.</td></tr>
<tr><td>A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.</td><td>A1.1.3 Examine customer privileges to verify each customer can only access resources allocated to them.</td></tr>
<tr><td>Customized Approach Objective
Customers cannot impact resources allocated to other customers.</td><td></td></tr>
</table>

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	**A1.1.4** Examine the results from the most recent penetration test to verify that testing confirmed the effectiveness of logical separation controls used to separate customer environments.	Multi-tenant services providers are responsible for managing the segmentation between their customers. Without technical assurance that segmentation controls are effective, it is possible that changes to the service provider's technology would inadvertently create a vulnerability that could be exploited across all the service provider's customers.
Customized Approach Objective		**Good Practice**
Segmentation of customer environments from other environments is periodically validated to be effective.		Effectiveness of separation techniques can be confirmed by using service-provider-created temporary (mock-up) environments that represent customer environments and attempting to 1) access one temporary environment from another environment, and 2) access a temporary environment from the Internet.
Applicability Notes		
The testing of adequate separation between customers in a multi-tenant service provider environment is in addition to the penetration tests specified in Requirement 11.4.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer. • Log data and availability is consistent with PCI DSS Requirement 10.	**A1.2.1** Examine documentation and system configuration settings to verify the provider has enabled audit log capability for each customer environment in accordance with all elements specified in this requirement.	Log information is useful for detecting and troubleshooting security incidents and is invaluable for forensic investigations. Customers therefore need to have access to these logs. However, log information can also be used by an attacker for reconnaissance, and so a customer's log information must only be accessible by the customer that the log relates to.
Customized Approach Objective		
Log capability is available to all customers without affecting the confidentiality of other customers.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.	**A1.2.2** Examine documented procedures to verify that the provider has processes or mechanisms to support and/or facilitate a prompt forensic investigation of related servers in the event of a suspected or confirmed security incident for any customer.	In the event of a suspected or confirmed breach of confidentiality of cardholder data, a customer's forensic investigator aims to find the cause of the breach, exclude the attacker from the environment, and ensure all unauthorized access is removed. Prompt and efficient responses to forensic investigators' requests can significantly reduce the time taken for the investigator to secure the customer's environment.
Customized Approach Objective		
Forensic investigation is readily available to all customers in the event of a suspected or confirmed security incident.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	**A1.2.3** Examine documented procedures and interview personnel to verify that the provider has a mechanism for reporting and addressing suspected or confirmed security incidents and vulnerabilities, in accordance with all elements specified in this requirement.	Security vulnerabilities in the provided services can impact the security of all the service provider's customers and therefore must be managed in accordance with the service provider's established processes, with priority given to resolving vulnerabilities that have the highest probability of compromise. Customers are likely to notice vulnerabilities and security misconfigurations while using the service. Implementing secure methods for customers to report security incidents and vulnerabilities encourages customers to report potential issues and enable the provider to quickly learn about and address potential issues within their environment.
Customized Approach Objective		
Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.		
Applicability Notes		
This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections

Sections

A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.

Overview

This Appendix applies only to entities using SSL/early TLS as a security control to protect POS POI terminals, including service providers that provide connections into POS POI terminals.

Entities using SSL and early TLS for POS POI terminal connections must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment terminals. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether it is susceptible to any known exploits.

The PCI DSS requirements directly affected are:

- **Requirement 2.2.5**: Where any insecure services, protocols, or daemons are present; business justification is documented, and additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.
- **Requirement 2.2.7**: All non-console administrative access is encrypted using strong cryptography.
- **Requirement 4.2.1**: Strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks.

SSL and early TLS must not be used as a security control to meet these requirements, except in the case of POS POI terminal connections, as detailed in this appendix. To support entities working to migrate from SSL/early TLS on POS POI terminals, the following provisions are included:

- New POS POI terminal implementations must not use SSL or early TLS as a security control.
- All POS POI terminal service providers must provide a secure service offering.
- Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, **and the SSL/TLS termination points to which they connect**, may continue using SSL/early TLS as a security control.

Requirements in this Appendix are not eligible for the Customized Approach.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.		
Defined Approach Requirements **A2.1.1** Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols. **Customized Approach Objective** This requirement is not eligible for the customized approach. **Applicability Notes** This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS POI service providers. The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known risks. If new exploits are introduced to which POS POI terminals are susceptible, the POS POI terminals will need to be updated immediately.	**Defined Approach Testing Procedures** **A2.1.1** For POS POI terminals using SSL and/or early TLS, confirm the entity has documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	**Purpose** POS POI terminals used in card-present environments can continue using SSL/early TLS when it can be shown that the POS POI terminal is not susceptible to the currently known exploits. **Good Practice** However, SSL is outdated technology and could be susceptible to additional security vulnerabilities in the future; it is therefore strongly recommended that POS POI terminals be upgraded to a secure protocol as soon as possible. If SSL/early TLS is not needed in the environment, use of, and fallback to these versions should be disabled. **Further Information** Refer to the current PCI SSC Information Supplements on SSL/Early TLS for further guidance.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
A2.1.2 ***Additional requirement for service providers only:*** All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. • Risk-assessment results and risk-reduction controls in place. • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments. • Overview of migration project plan to replace SSL/early TLS at a future date.	**A2.1.2** ***Additional testing procedure for service provider assessments only:*** Review the documented Risk Mitigation and Migration Plan to verify it includes all elements specified in this requirement.	**Purpose** POS POI termination points, including but not limited to service providers such as acquirers or acquirer processors, can continue using SSL/early TLS when it can be shown that the service provider has controls in place that mitigate the risk of supporting those connections for the service provider environment. **Good Practice** Service providers should communicate to all customers using SSL/early TLS about the risks associated with its use and the need to migrate to a secure protocol. **Definitions** The Risk Mitigation and Migration Plan is a document prepared by the entity that details its plans for migrating to a secure protocol and describes controls the entity has in place to reduce the risk associated with SSL/early TLS until the migration is complete. **Further Information** Refer to the current PCI SSC Information Supplements on SSL/early TLS for further guidance on Risk Mitigation and Migration Plans.
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Customers must be able to choose to upgrade their POIs to eliminate the vulnerability in using SSL and early TLS. In many cases, customers will need to take a phased or gradual approach to migrate their POS POI estate from the insecure protocol to a secure protocol and so will require the service provider to support a secure offering. **Further Information** Refer to the current PCI SSC Information Supplements on SSL/Early TLS for further guidance.
A2.1.3 ***Additional requirement for service providers only***: All service providers provide a secure service offering.	**A2.1.3** ***Additional testing procedure for service provider assessments only:*** Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for its service.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix A3: Designated Entities Supplemental Validation (DESV)

Sections

A3.1 A PCI DSS compliance program is implemented.

A3.2 PCI DSS scope is documented and validated.

A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.

A3.4 Logical access to the cardholder data environment is controlled and managed.

A3.5 Suspicious events are identified and responded to.

Overview

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. An entity is required to undergo an assessment according to this Appendix ONLY if instructed to do so by an acquirer or a payment brand. Examples of entities that this Appendix could apply to include:

- Those storing, processing, and/or transmitting large volumes of account data,
- Those providing aggregation points for account data, or
- Those that have suffered significant or repeated breaches of account data.

Additionally, other PCI standards may reference completion of this Appendix.

These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes and increased validation and scoping consideration.

(continued on next page)

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

(continued)

***Note**: Some PCI DSS requirements in this Appendix have defined timeframes (for example, an activity that is to be performed at least once every three months or six months). For an initial assessment to such requirements, it is not required that an activity has been performed for every such timeframe during the previous year, if the assessor verifies:*

- *The activity was performed in accordance with the applicable requirement within the most recent timeframe (for example, the most recent three-month or six-month period), and*
- *The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.*

For subsequent years after the initial assessment, an activity must have been performed within each required timeframe. For example, an activity required at least every three months must have been performed at least four times during the previous year at an interval that does not exceed 90-92 days.

Refer to section 7 Descriptions of Timeframes Used in PCI DSS Requirements *for additional guidance about initial assessments.*

Not all requirements in PCI DSS apply to all entities that may undergo a PCI DSS assessment. It is for this reason that some PCI DSS Requirements are duplicated in this appendix. Any questions about this appendix should be addressed to acquirers or payment brands.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A3.1 A PCI DSS compliance program is implemented.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. **Good Practice** Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.
A3.1.1 Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program. • Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months. **PCI DSS Reference**: *Requirement 12*	**A3.1.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance. **A3.1.1.b** Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized. **A3.1.1.c** Examine executive management and board of directors meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least once every 12 months.	
Customized Approach Objective		
This requirement is not eligible for the customized approach		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
A3.1.2 A formal PCI DSS compliance program is in place that includes: • Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities. • Annual PCI DSS assessment processes. • Processes for the continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. **PCI DSS Reference**: *Requirements 1-12*	**A3.1.2.a** Examine information security policies and procedures to verify that processes are defined for a formal PCI DSS compliance program that includes all elements specified in this requirement.	**Purpose** A formal compliance program allows an organization to monitor the health of its security controls, be proactive if a control fails, and effectively communicate activities and compliance status throughout the organization. **Good Practice** The PCI DSS compliance program can be a dedicated program or part of overarching compliance and/or governance program, and should include a well-defined methodology that demonstrates consistent and effective evaluation. Strategic business decisions that should be analyzed for potential PCI DSS impacts may include mergers and acquisitions, new technology purchases, or new payment-acceptance channels. **Definitions** Maintaining and monitoring an organization's overall PCI DSS compliance includes identifying activities to be performed daily, weekly, monthly, every three months, or annually, and ensuring these activities are being performed accordingly (for example, using a security self-assessment or PDCA methodology). **Examples** Methodologies that support the management of compliance programs include Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, and Six Sigma.
Customized Approach Objective	**A3.1.2.b** Interview personnel and observe compliance activities to verify that a formal PCI DSS compliance program is implemented in accordance with all elements specified in this requirement.	
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The formal definition of specific PCI DSS compliance roles and responsibilities helps to ensure accountability and monitoring of ongoing PCI DSS compliance efforts. **Good Practice** Ownership should be assigned to individuals with the authority to make risk-based decisions, and upon whom accountability rests for the specific function. Duties should be formally defined, and owners should be able to demonstrate an understanding of their responsibilities and accountability. Compliance roles may be assigned to a single owner or multiple owners for different requirement elements.
A3.1.3 PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including: • Managing PCI DSS business-as-usual activities. • Managing annual PCI DSS assessments. • Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. **PCI DSS Reference**: *Requirement 12*	**A3.1.3.a** Examine information security policies and procedures and interview personnel to verify that PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel in accordance with all elements of this requirement.	
	A3.1.3.b Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Personnel responsible for PCI DSS compliance have specific training needs exceeding that which is typically provided by general security awareness training to enable them to perform their role. **Good Practice** Individuals with PCI DSS compliance responsibilities should receive specialized training that, in addition to a general awareness of information security, focuses on specific security topics, skills, processes, or methodologies that must be followed for those individuals to perform their compliance responsibilities effectively. Training may be offered by third parties such as the PCI SSC (for example, PCI Awareness, PCIP, and ISA), payment brands, and acquirers, or training may be internal. Training content should be applicable for the individual's job function, be current, and include the latest security threats and/or version of PCI DSS. **Further Information** For additional guidance, refer to *Information Supplement: Best Practices for Implementing a Security Awareness Program*.
A3.1.4 Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). **PCI DSS Reference**: *Requirement 12*	**A3.1.4.a** Examine information security policies and procedures to verify that PCI DSS and/or information security training is required at least once every 12 months for each role with PCI DSS compliance responsibilities.	
Customized Approach Objective	**A3.1.4.b** Interview personnel and examine certificates of attendance or other records to verify that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least once every 12 months.	
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A3.2 PCI DSS scope is documented and validated.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	
A3.2.1 PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. *(continued on next page)*	**A3.2.1.a** Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every three months. • After significant changes to the in-scope environment. **A3.2.1.b** Examine documented results of scope reviews occurring at least once every three months to verify that scoping validation includes all elements specified in this requirement.	**Purpose** Frequent validation of PCI DSS scope helps to ensure PCI DSS scope remains up to date and aligned with changing business objectives, and therefore that security controls are protecting all appropriate system components. **Good Practice** Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information: • Data stores (databases, files, cloud, etc.), including purpose of data storage and the retention period, • Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization), • How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization), • How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.). *(continued on next page)*

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
• Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope • Identifying all connections to third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. **PCI DSS Reference**: *Scope of PCI DSS Requirements, Requirement 12.* **Customized Approach Objective** This requirement is not eligible for the customized approach.		In addition to internal systems and networks, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls can be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE. A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured. **Further Information** Refer to *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* for additional guidance.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Changes to systems or networks can have a significant impact on PCI DSS scope. For example, changes to network security control rulesets can bring whole network segments into scope, or new systems may be added to the CDE that have to be appropriately protected. A formal impact assessment performed in advance of a change gives the entity assurance that the change will not adversely affect the security of the CDE. **Good Practice** Processes to determine the potential impact that changes to systems and networks may have on an entity's PCI DSS scope may be performed as part of a dedicated PCI DSS compliance program or may fall under an entity's overarching compliance and/or governance program.
A3.2.2 PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: • Performing a formal PCI DSS impact assessment. • Identifying applicable PCI DSS requirements to the system or network. • Updating PCI DSS scope as appropriate. • Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). **PCI DSS Reference**: *Scope of PCI DSS Requirements; Requirements 1-12*	**A3.2.2** Examine change documentation and interview personnel to verify that for each change to systems or networks the PCI DSS scope impact is determined, and includes all elements specified in this requirement.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to have processes to analyze all changes made to systems or networks, to ensure that all appropriate PCI DSS controls are applied to any systems or networks added to the in-scope environment due to a change. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date, and security controls are applied where needed. **Good Practice** A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through an iterative process. **Examples** PCI DSS requirements that should be verified include, but are not limited to: • Network diagrams are updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—for example, file integrity monitoring, antimalware, patches, and audit logging. • Sensitive authentication data is not stored, and all account data storage is documented and incorporated into data-retention policy and procedures. • New systems are included in the quarterly vulnerability scanning process.
A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. **PCI DSS Reference**: *Scope of PCI DSS Requirements; Requirement 1-12*	**A3.2.2.1** Examine change records and the affected systems/networks, and interview personnel to verify that all relevant PCI DSS requirements were confirmed to be implemented and documentation updated as part of the change.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported PCI DSS controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit PCI DSS scope and controls when there are changes to an organization's structure and management to ensure controls are in place and active. **Examples** Changes to organizational structure include, but are not limited to, company mergers or acquisitions, and significant changes or reassignments of personnel with responsibility for security control.
A3.2.3 Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. **PCI DSS Reference**: *Requirement 12*	**A3.2.3** Examine policies and procedures to verify that a change to organizational structure results in formal a review of the impact on PCI DSS scope and applicability of controls.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** PCI DSS normally requires segmentation controls to be verified by penetration testing every twelve months. Validating segmentation controls more frequently is likely to discover failings in segmentation before they can be exploited by an attacker attempting to pivot laterally from an out-of-scope untrusted network to the CDE. **Good Practice** Although the requirement specifies that this scope validation is carried out at least once every six months and after a significant change, this exercise should be performed as frequently as possible to ensure it remains effective at isolating the CDE from other networks. **Further Information** Refer to *Information Supplement: Penetration Testing Guidance* for additional guidance.
A3.2.4 If segmentation is used, PCI DSS scope is confirmed as follows: • Per the entity's methodology defined at Requirement 11.4.1. • Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. **PCI DSS Reference**: *Requirement 11*	**A3.2.4** Examine the results from the most recent penetration test to verify that the test was conducted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
A3.2.5 A data-discovery methodology is implemented that: • Confirms PCI DSS scope. • Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. • Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. **PCI DSS Reference**: *Scope of PCI DSS Requirements*	**A3.2.5.a** Examine the documented data-discovery methodology to verify it includes all elements specified in this requirement. **A3.2.5.b** Examine results from recent data discovery efforts, and interview responsible personnel to verify that data discovery is performed at least once every three months and upon significant changes to the CDE or processes.	**Purpose** PCI DSS requires that, as part of the scoping exercise, assessed entities must identify and document the existence of all cleartext PAN in their environments. Implementing a data-discovery methodology that identifies all sources and locations of cleartext PAN and looks for cleartext PAN on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file— helps to ensure that previously unknown locations of cleartext PAN are detected and properly secured. **Examples** A data-discovery process can be performed via a variety of methods, including, but not limited to 1) commercially available data-discovery software, 2) an in-house developed data-discovery program, or 3) a manual search. A combination of methodologies may also be used as needed. Regardless of the method used, the goal of the effort is to find all sources and locations of cleartext PAN (not just in the defined CDE).
Customized Approach Objective		
This requirement is not eligible for the customized approach		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A process to test the effectiveness of the methods used for data discovery ensures the completeness and accuracy of account data detection. **Good Practice** For completeness, system components in the in-scope networks, and systems in out-of-scope networks, should be included in the data-discovery process. The data-discovery process should be effective on all operating systems and platforms in use. Accuracy can be tested by placing test PANs on system components and file formats in use and confirming that the data-discovery method detected the test PANs.
A3.2.5.1 Data discovery methods are confirmed as follows: • Effectiveness of methods is tested. • Methods are able to discover cleartext PAN on all types of system components and file formats in use. • The effectiveness of data-discovery methods is confirmed at least once every 12 months. **PCI DSS Reference**: *Scope of PCI DSS Requirements*	**A3.2.5.1.a** Interview personnel and review documentation to verify: • The entity has a process in place to test the effectiveness of methods used for data discovery. • The process includes verifying the methods are able to discover cleartext PAN on all types of system components and file formats in use.	
Customized Approach Objective	**A3.2.5.1.b** Examine the results of effectiveness tests to verify that the effectiveness of data-discovery methods is confirmed at least once every 12 months.	
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Having documented response procedures that are followed in the event cleartext PAN is found outside the CDE helps to identify the necessary remediation actions and prevent future leaks. **Good Practice** If PAN was found outside the CDE, an analysis should be performed to 1) determine whether it was saved independently of other data or with sensitive authentication data, 2) to identify the source of the data, and 3) identify the control gaps that resulted in the data being outside the CDE. Entities should consider whether contributory factors, such as business processes, user behavior, improper system configurations, etc., caused the PAN to be stored in an unexpected location. If such contributory factors are present, they should be addressed per this Requirement to prevent a recurrence.
A3.2.5.2 Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include: • Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Determining how the data ended up outside the CDE. • Remediating data leaks or process gaps that resulted in the data being outside the CDE. • Identifying the source of the data. • Identifying whether any track data is stored with the PANs.	**A3.2.5.2.a** Examine documented response procedures to verify that procedures for responding to the detection of cleartext PAN outside the CDE are defined and include all elements specified in this requirement.	
	A3.2.5.2.b Interview personnel and examine records of response actions to verify that remediation activities are performed when cleartext PAN is detected outside the CDE.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The use of mechanisms to detect and prevent unauthorized PAN from leaving the CDE allows an organization to detect and prevent situations that may lead to data loss. **Good Practice** Coverage of the mechanisms should include, but not be limited to, e-mails, downloads to removable media, and output to printers. **Examples** Mechanisms to detect and prevent unauthorized loss of cleartext PAN may include the use of appropriate tools such as data loss prevention (DLP) solutions as well as manual processes and procedures.
A3.2.6 Mechanisms are implemented for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including mechanisms that are: • Actively running. • Configured to detect and prevent cleartext PAN leaving the CDE via an unauthorized channel, method, or process. • Generating audit logs and alerts upon detection of cleartext PAN leaving the CDE via an unauthorized channel, method, or process. **PCI DSS Reference**: *Scope of PCI DSS Requirements, Requirement 12*	**A3.2.6.a** Examine documentation and observe implemented mechanisms to verify that the mechanisms are in accordance with all elements specified in this requirement.	
	A3.2.6.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. **PCI DSS Reference**: *Requirement 12*	**A3.2.6.1.a** Examine documented response procedures to verify that procedures for responding to the attempted removal of cleartext PAN from the CDE via an unauthorized channel, method, or process include all elements specified in this requirement: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss.	Attempts to remove cleartext PAN via an unauthorized channel, method, or process may indicate malicious intent to steal data, or may be the actions of an authorized employee who is unaware of or simply not following the proper methods. Prompt investigation of these occurrences can identify where remediation needs to be applied and provides valuable information to help understand from where the threats are coming.
Customized Approach Objective	**A3.2.6.1.b** Interview personnel and examine records of actions taken when cleartext PAN is detected leaving the CDE via an unauthorized channel, method, or process and verify that remediation activities were performed.	
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Without formal processes for the prompt (as soon as possible) detection, alerting, and addressing of critical security control failures, failures may go undetected or remain unresolved for extended periods. In addition, without formalized time-bound processes, attackers will have ample time to compromise systems and steal account data from the CDE. **Good Practice** The specific types of failures may vary, depending on the function of the device system component and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner, such as a firewall erasing all its rules or going offline.
A3.3.1 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: • Network security controls • IDS/IPS • FIM • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) • Automated audit log review mechanisms. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Automated code review tools (if used). *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* **PCI DSS Reference**: *Requirements 1-12*	**A3.3.1.a** Examine documented policies and procedures to verify that processes are defined to promptly detect, alert, and address critical security control failures in accordance with all elements specified in this requirement.	
	A3.3.1.b Examine detection and alerting processes, and interview personnel to verify that processes are implemented for all critical security controls specified in this requirement and that each failure of a critical security control results in the generation of an alert.	
Customized Approach Objective		
This requirement is not eligible for the customized approach. *(continued on next page)*		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Applicability Notes *The bullets above (for automated log review mechanisms and automated code review tools (if used)) are best practices until 31 March 2025, after which they will be required as part of Requirement A3.3.1 and must be fully considered during a PCI DSS assessment.*		
Defined Approach Requirements **A3.3.1.1** Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. **PCI DSS Reference**: *Requirements 1-12*	**Defined Approach Testing Procedures** **A3.3.1.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond promptly to a security control failure in accordance with all elements specified in this requirement. **A3.3.1.1.b** Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause. • Duration (date and time start and end) of the security failure. • Details of the remediation required to address the root cause.	**Purpose** If alerts from failures of critical security control systems are not responded to quickly and effectively, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. **Good Practice** Documented evidence (for example, records within a problem management system) should support processes and procedures in place that respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.
Customized Approach Objective This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="5">Purpose
Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies. Conducting appropriate reviews of these technologies ensures that they can prepare for, and manage, vulnerabilities in hardware and software that will not be remediated by the vendor or developer.
Good Practice
Organizations should also consider reviewing firmware versions to ensure they remain current and supported by the vendors.
Organizations also need to be aware of changes made by technology vendors to their products or processes to understand how such changes may impact the organization’s use of the technology.
Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies and ensure controls that rely on those technologies remain effective. These reviews include, but are not limited to, reviewing technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.</td></tr>
<tr><td rowspan="3">A3.3.2 Hardware and software technologies are reviewed at least once every 12 months to confirm whether they continue to meet the organization’s PCI DSS requirements.
PCI DSS Reference: Requirements 2, 6, 12.</td><td>A3.3.2.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization’s PCI DSS requirements.</td></tr>
<tr><td>A3.3.2.b Review the results of the recent reviews of hardware and software technologies to verify reviews are performed at least once every 12 months.</td></tr>
<tr><td rowspan="3">A3.3.2.c Review documentation to verify that, for any technologies that have been determined to no longer meet the organization’s PCI DSS requirements, a plan is in place to remediate the technology.</td></tr>
<tr><td>Customized Approach Objective</td></tr>
<tr><td>This requirement is not eligible for the customized approach.</td></tr>
<tr><td>Applicability Notes</td><td></td></tr>
<tr><td>The process includes a plan for remediating technologies that no longer meet the organization’s PCI DSS requirements, up to and including replacement of the technology, as appropriate.</td><td></td></tr>
</table>

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	
A3.3.3 Reviews are performed at least once every three months to verify BAU activities are being followed. Reviews are performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include: • Confirmation that all BAU activities, including A3.2.2, A3.2.6, and A3.3.1, are being performed. • Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, ruleset reviews for network security controls, configuration standards for new systems). • Documenting how the reviews were completed, including how all BAU activities were verified as being in place. • Collection of documented evidence as required for the annual PCI DSS assessment. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program, as identified in A3.1.3. • Retention of records and documentation for at least 12 months, covering all BAU activities. **PCI DSS Reference**: *Requirements 1-12*	**A3.3.3.a** Examine policies and procedures to verify that processes are defined for reviewing and verifying BAU activities in accordance with all elements specified in this requirement.	**Purpose** Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to reperform other PCI DSS requirements, but to confirm that security activities are being performed on an ongoing basis. **Good Practice** These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, reviews of network security control rulesets—to assist in the entity's preparation for its next PCI DSS assessment. **Examples** Looking at Requirement 1.2.7 as one example, Requirement A3.3.3 is met by confirming, at least once every three months, that reviews of configurations of network security controls have occurred at the required frequency. On the other hand, Requirement 1.2.7 is met by reviewing those configurations as specified in the requirement.
	A3.3.3.b Interview responsible personnel and examine records of reviews to verify that: • Reviews are performed by personnel assigned to the PCI DSS compliance program. • Reviews are performed at least once every three months.	
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A3.4 Logical access to the cardholder data environment is controlled and managed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
A3.4.1 User accounts and access privileges to in-scope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized. **PCI DSS Reference**: *Requirement 7*	**A3.4.1** Interview responsible personnel and examine supporting documentation to verify that: • User accounts and access privileges are reviewed at least every six months. • Reviews confirm that access is appropriate based on job function and that all access is authorized.	Regular review of access rights helps to detect excessive access rights remaining after user job responsibilities change, system functions change, or other modifications. If excessive user rights are not revoked in due time, they may be used by malicious users for unauthorized access. This review provides another opportunity to ensure that accounts for all terminated users have been removed (if any were missed at the time of termination), as well as to ensure that any third parties that no longer need access have had their access terminated.
Customized Approach Objective		
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Requirements and Testing Procedures		Guidance
A3.5 Suspicious events are identified and responded to.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** The ability to identify attack patterns and undesirable behavior across systems—for example, using centrally managed or automated log-correlation tools— is critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something goes wrong. Determining the cause of a compromise is very difficult, if not impossible, without a process to corroborate information from critical system components and systems that perform security functions, such as network security controls, IDS/IPS, and file integrity monitoring (FIM) systems. Thus, logs for all critical system components and systems that perform security functions need to be collected, correlated, and maintained. This could include using software products and service methodologies to provide real-time analysis, alerting, and reporting, such as security information and event management (SIEM), FIM, or change detection.
A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures. **PCI DSS Reference**: *Requirements 10, 12*	**A3.5.1.a** Examine documentation and interview personnel to verify a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a prompt manner, and includes all elements specified in this requirement.	
Customized Approach Objective	**A3.5.1.b** Examine incident response procedures and interview responsible personnel to verify that: • On-call personnel receive prompt alerts. • Alerts are responded to per documented response procedures.	
This requirement is not eligible for the customized approach.		

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix B Compensating Controls

Compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as stated, due to legitimate and documented technical or business constraints but has sufficiently mitigated the risk associated with not meeting the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. To understand the intent of a requirement, see *the Customized Approach Objective* for most PCI DSS requirements. If a requirement is not eligible for the Customized Approach and therefore does not have a Customized Approach Objective, refer to the **Purpose** in the Guidance column for that requirement.
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. When evaluating "above and beyond" for compensating controls, consider the following:
    a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting cleartext administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of cleartext passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).
    b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area but are not required for the item under review.
    c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to address a vulnerability that is exploitable through a network interface because a security update is not yet available from a vendor, a compensating control could consist of controls that include all of the following: 1) internal network segmentation, 2) limiting network access to the vulnerable interface to only required devices (IP address or MAC address filtering), and 3) IDS/IPS monitoring of all traffic destined to the vulnerable interface.

Note: *All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS assessment. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a given compensating control will not be effective in all environments.*

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

5. Address the additional risk imposed by not adhering to the PCI DSS requirement.
6. Address the requirement currently and in the future. A compensating control cannot address a requirement that was missed in the past (for example, where performance of a task was required two quarters ago, but that task was not performed).

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to confirm that each compensating control adequately addresses the risk that the original PCI DSS requirement was designed to address, per items 1-6 above.

To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete. Additionally, compensating control results must be documented in the applicable report for the assessment (for example, a Report on Compliance or a Self-Assessment Questionnaire) in the corresponding PCI DSS requirement section, and included when the applicable report is submitted to the requesting organization.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix C Compensating Controls Worksheet

The entity must use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in accordance with instructions in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: *Only entities that have legitimate and documented technological or business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control (for example, the Customized Approach Objective).	
	Identify the objective met by the compensating control *(note: this can be, but is not required to be, the stated Customized Approach Objective for the PCI DSS requirement).*	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix D Customized Approach

This approach is intended for entities that decide to meet a PCI DSS requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. The customized approach allows an entity to take a strategic approach to meeting a requirement's Customized Approach Objective, so it can determine and design the security controls needed to meet the objective in a manner unique for that organization.

The entity implementing a customized approach must satisfy the following criteria:

- Document and maintain evidence about each customized control, including all information specified in the Controls Matrix Template in *PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website
- Perform and document a targeted risk analysis (PCI DSS Requirement 12.3.2) for each customized control, including all information specified in the Targeted Risk Analysis Template in *PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website.
- Perform testing of each customized control to prove effectiveness, and document testing performed, methods used, what was tested, when testing was performed, and results of testing in the controls matrix.
- Monitor and maintain evidence about the effectiveness of each customized control.
- Provide completed controls matrix(es), targeted risk analysis, testing evidence, and evidence of customized control effectiveness to its assessor.

The assessor performing an assessment of customized controls must satisfy the following criteria:

- Review the entity's controls matrix(es), targeted risk analysis, and evidence of control effectiveness to fully understand the customized control(s) and to verify the entity meets all Customized Approach documentation and evidence requirements.
- Derive and document the appropriate testing procedures needed to conduct thorough testing of each customized control.
- Test each customized control to determine whether the entity's implementation 1) meets the requirement's Customized Approach Objective and 2) results in an "in place" finding for the requirement.
- At all times, QSAs maintain independence requirements defined in the QSA Qualification Requirements. This means if a QSA is involved in designing or implementing a customized control, that QSA does not also derive testing procedures for, assess, or assist with the assessment of that customized control.

The entity and its assessor are expected to work together to ensure 1) they agree that the customized control(s) fully meets the customized approach objective, 2) the assessor fully understands the customized control, and 3) the entity understands the derived testing the assessor will perform.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Use of the customized approach must be documented by a QSA or ISA in accordance with instructions in the Report on Compliance (ROC) Template and following the instructions in the *FAQs for use with PCI DSS v4.x ROC Template* available on the PCI SSC website.

Entities that complete a Self-Assessment Questionnaire are not eligible to use a customized approach; however, these entities may elect to have a QSA or ISA perform their assessment and document it in a ROC Template.

The use of the customized approach may be regulated by organizations that manage compliance programs (for example, payment brands and acquirers). Therefore, questions about use of a customized approach must be referred to those organizations, including, for example, whether an entity is required to use a QSA, or may use an ISA to complete an assessment using the customized approach.

Note: *Compensating controls are not an option with the customized approach. Because the customized approach allows an entity to determine and design the controls needed to meet a requirement's Customized Approach Objective, the entity is expected to effectively implement the controls it designed for that requirement without needing to also implement alternate, compensating controls.*

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix E Sample Templates to Support Customized Approach

Sample templates to support the Customized Approach (the *Sample Controls Matrix Template* and *Sample Targeted Risk Analysis Template*) provide examples of formats that could be used by entities when documenting their Customized Approach. *While it is not required that entities follow the specific formats provided in these sample templates, the entity's control matrix and targeted risk analysis must include all the information as defined in these templates.*

These sample templates are available on the PCI SSC website.

© 2006 -2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix F Leveraging the PCI Software Security Framework to Support Requirement 6

PCI DSS Requirement 6 defines requirements for the development and maintenance of secure systems and software. Because the PCI SSC Secure Software Standard and the Secure SLC Standard (collectively, the Software Security Framework) include rigorous software security requirements, the use of bespoke and custom software that is developed and maintained in accordance with either standard can help the entity to meet several requirements in PCI DSS Requirement 6 without having to perform additional detailed testing, and may also support use of the Customized Approach for other requirements. For details, see Table 7.

***Note**: This support for meeting Requirement 6 applies only to software that is specifically developed and maintained in accordance with the Secure Software Standard or the Secure SLC Standard; it does not extend to other software or system components in scope for Requirement 6.*

Table 7. Leveraging the PCI Software Security Framework to Support Requirement 6

PCI DSS Requirements	How PCI DSS Requirements Apply to Software Developed and Maintained in Accordance with the Secure Software Standard	How PCI DSS Requirements Apply to Software Developed and Maintained in Accordance with the Secure SLC Standard
6.1 Processes and mechanisms for performing activities in Requirement 6 are defined and understood.	PCI DSS requirements/objectives apply as usual.	
6.2 Bespoke and custom software is developed securely.	PCI DSS Requirement 6.2.4 can be considered in place for software that is developed and maintained in accordance with the Secure Software Standard.	PCI DSS Requirement 6.2 can be considered in place for software that is developed and maintained in accordance with the Secure SLC Standard.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

PCI DSS Requirements	How PCI DSS Requirements Apply to Software Developed and Maintained in Accordance with the Secure Software Standard	How PCI DSS Requirements Apply to Software Developed and Maintained in Accordance with the Secure SLC Standard
6.3 Security vulnerabilities are identified and addressed.	PCI DSS requirements/objectives apply as usual. Software developed and maintained in accordance with the Secure SLC Standard may support the customized approach for Requirement 6.3 objectives. While use of software developed and maintained in accordance with the Secure SLC Standard provides assurance that the vendor makes security patches and software updates available in a timely manner, **the entity retains responsibility** for ensuring that patches and updates are installed in accordance with PCI DSS requirements.	
6.4 Public-facing web applications are protected against attacks.	PCI DSS requirements/objectives apply as usual.	
6.5 Changes to all system components are managed securely.	PCI DSS requirements/objectives apply as usual. Software developed and maintained in accordance with the Secure SLC Standard may support the customized approach for Requirement 6.5 objectives. While use of software developed and maintained in accordance with the Secure SLC Standard provides assurance that the vendor follows change management procedures during development of software and related updates, **the entity retains responsibility** for ensuring that software and other changes to system components are implemented into its production environment in accordance with PCI DSS requirements.	

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Use of Bespoke and Custom Software Developed and Maintained by a Secure SLC Qualified Vendor

When validating the use of software developed and maintained by a Secure SLC Qualified Vendor to meet PCI DSS Requirement 6.2 and support the Customized Approach for Requirements 6.3 and 6.5, the assessor must confirm that the following is met:

- The software vendor has a current listing on the PCI SSC List of Secure SLC Qualified Vendors—that is, the validation has not expired.
- The software was developed and is being maintained using software lifecycle management practices that were assessed as part of the software vendor's validation.
- The entity is following the implementation guidance provided by the Secure SLC Qualified Vendor.

Use of Bespoke and Custom Software Developed in Accordance with the Secure SLC Standard

Entities that internally develop software solely for their use or that develop software for use by a single entity may choose to engage a Secure SLC Assessor to assess their software lifecycle management practices against the Secure SLC Standard. The Secure SLC Assessor will document the results of the assessment in a Secure SLC Report on Compliance (ROC) and a Secure SLC Attestation of Compliance (AOC).

Software that is developed and maintained following software lifecycle management practices provides the same support for PCI DSS Requirement 6 as software developed and maintained by a Secure SLC Qualified Vendor, if those practices were assessed by a Secure SLC Assessor and confirmed to meet the Secure SLC Standard requirements, with the results documented in a Secure SLC ROC and AOC.

Validating the Use of the Secure SLC Standard

When validating the use of software developed and maintained in accordance with the Secure SLC Standard to meet PCI DSS Requirement 6.2 and support customized approach for Requirements 6.3 and 6.5, the assessor must confirm that the following are met:

- The software lifecycle management practices were assessed by a Secure SLC Assessor and confirmed to meet all Secure SLC Standard requirements with the results documented in a Secure SLC Report on Compliance (ROC) and Secure SLC Attestation of Compliance (AOC).
- The software was developed and maintained using the software lifecycle management practices covered by the Secure SLC assessment.
- A full Secure SLC assessment of the software lifecycle management practices was completed within the previous 36 months. Additionally, if the most recent full Secure SLC assessment occurred more than 12 months ago, an Annual Attestation was provided by the developer/vendor within the previous 12 months that confirms continued adherence to Secure SLC Standard for the software lifecycle management practices in use.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Validating the Use of the Secure Software Standard

When validating the use of software developed and maintained in accordance with the Secure Software Standard to meet PCI DSS Requirement 6.2.4 and support customized approach for Requirements 6.3 and 6.5, the assessor must confirm that the following are met:

- The secure software assessment was conducted by a Secure Software Assessor and confirmed to meet all requirements in the Secure Software Standard with the results documented in a Secure Software Report on Validation (ROV) and Secure Software Attestation of Validation (AOV).
- The software was developed and is being maintained using the software lifecycle management practices that were covered by the Secure Software assessment.
- A full Secure Software assessment was completed within the previous 36 months. Additionally, if the most recent full Secure Software assessment occurred more than 12 months ago, an Annual Attestation was provided by the developer/vendor within the previous 12 months that confirms continued adherence to Secure Software Standard.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Term	Definition
Account	Also referred to as "user ID," "account ID," or "application ID." Used to identify an individual or process on a computer system. See *Authentication Credentials* and *Authentication Factor*.
Account Data	Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data*.
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See *Payment Processor*.
Administrative Access	Elevated or increased privileges granted to an account for that account to manage systems, networks, and/or applications. Administrative access can be assigned to an individual's account or a built-in system account. Accounts with administrative access are often referred to as "superuser," "root," "administrator," "admin," "sysadmin," or "supervisor-state," depending on the particular operating system and organizational structure.
AES	Acronym for "Advanced Encryption Standard." See *Strong Cryptography.*
ANSI	Acronym for "American National Standards Institute."
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
AOC	Acronym for "Attestation of Compliance." The AOC is the official PCI SSC form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC).
Application	Includes all purchased, custom, and bespoke software programs or groups of programs, including both internal and external (for example, web) applications.
Application and System Accounts	Also referred to as "service accounts." Accounts that execute processes or perform tasks on a computer system or in an application. These accounts usually have elevated privileges that are required to perform specialized tasks or functions and are not typically accounts used by an individual.
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs with one or more authentication factors. See *Account, Authentication Credential,* and *Authentication Factor.*
Authentication Credential	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process. See *Account* and *Authentication Factor.*
Authentication Factor	The element used to prove or verify the identity of an individual or process on a computer system. Authentication typically occurs with one or more of the following authentication factors: • Something you know, such as a password or passphrase, • Something you have, such as a token device or smart card, • Something you are, such as a biometric element. The ID (or account) and authentication factor together are considered authentication credentials. See *Account* and *Authentication Credential.*
Authorization	In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization refers to the authorization process, which completes when a merchant receives a transaction response (for example, an approval or decline).
BAU	Acronym for "Business as Usual."
Bespoke and Custom Software	*Bespoke software* is developed for the entity by a third party on the entity's behalf and per the entity's specifications. *Custom software* is developed by the entity for its own use.
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
Card Verification Code	Also referred to as Card Validation Code or Value, or Card Security Code. For PCI DSS purposes, it is the three- or four-digit value printed on the front or back of a payment card. May be referred to as CAV2, CVC2, CVN2, CVV2, or CID according to the individual Participating Payment Brands. For more information, contact the Participating Payment Brands.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Cardholder	Customer to which a payment card is issued, or any individual authorized to use the payment card. See *Visitor.*
Cardholder Data (CHD)	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See *Sensitive Authentication Data* for additional data elements that might be transmitted or processed (but not stored) as part of a payment transaction.
CDE	Acronym for "Cardholder Data Environment." The CDE is comprised of: • The system components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and, • System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.
CERT	Acronym for "Computer Emergency Response Team."
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.
CIS	Acronym for "Center for Internet Security."
Cleartext Data	Unencrypted data.
Column-Level Database Encryption	Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see *Disk Encryption* and *File-Level Encryption*.
Commercial Off-the-Shelf (COTS)	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Compensating Controls	See PCI DSS Appendices B and C.
Compromise	Also referred to as "data compromise" or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Console	Directly connected screen and/or keyboard which permits access and control of a server, mainframe computer, or other system type. See *Non-Console Access*.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Consumer	Individual cardholder purchasing goods, services, or both.
Critical systems	A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data.
Cryptographic Algorithm	Also referred to as "encryption algorithm." A clearly specified reversible mathematical process used for transforming cleartext data to encrypted data, and vice versa. See *Strong Cryptography.*
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that is used for operations such as: • Transforming cleartext data into ciphertext data, • Transforming ciphertext data into cleartext data, • A digital signature computed from data, • Verifying a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret. See *Strong Cryptography.*
Cryptographic Key Generation	Key generation is one of the functions within key management. The following documents provide recognized guidance on proper key generation: • *NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation* • *ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle* – 4.3 Key generation • *ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle* – 6.2 Key life cycle stages — Generation • *European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management* – 4.1.1 Key generation [for symmetric algorithms] – 4.2.1 Key generation [for asymmetric algorithms].
Cryptographic Key Management	The set of processes and mechanisms which support cryptographic key establishment and maintenance, including replacing older keys with new keys as necessary.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Cryptoperiod	The time span during which a cryptographic key can be used for its defined purpose. Often defined in terms of the period for which the key is active and/or the amount of ciphertext that has been produced by the key, and according to industry best practices and guidelines (for example, *NIST Special Publication 800-57*).
Customized Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
CVSS	Acronym for "Common Vulnerability Scoring System." Refer to *ASV Program Guide* for more information.
Data-Flow Diagram	A diagram showing how and where data flows through an entity's applications, systems, networks, and to/from external parties.
Default Account	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Defined Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
Disk Encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network.
DNS	Acronym for "Domain Name System."
Dual Control	Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. See *Split Knowledge*.
ECC	Acronym for "Elliptic Curve Cryptography." See *Strong Cryptography*.
E-commerce (web) Redirection Server	A server that redirects a customer browser from a merchant's website to a different location for payment processing during an ecommerce transaction.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Encryption	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data. See *Strong Cryptography*.
Encryption Algorithm	See *Cryptographic Algorithm*.
Entity	In the context of a PCI DSS assessment, a term used to represent the corporation, organization, or business which is undergoing an assessment.
File Integrity Monitoring (FIM)	A change-detection solution that checks for changes, additions, and deletions to critical files, and notifies when such changes are detected.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see *Disk Encryption* and *Column-Level Database Encryption*.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises. Investigations into compromises of payment data are typically conducted by a PCI Forensic Investigator (PFI).
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in cleartext. FTP can be implemented securely via SSH or other technology.
Hashing	A method to protect data that converts data into a fixed-length message digest. Hashing is a one-way (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). Hash functions are required to have the following properties: • It is computationally infeasible to determine the original input given only the hash code, • It is computationally infeasible to find two inputs that give the same hash code.
HSM	Acronym for "hardware security module" or "host security module." A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data.
IDS	Acronym for "intrusion-detection system."

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Index Token	A random value from a table of random values that corresponds to a given PAN.
Interactive Login	The process of an individual providing authentication credentials to directly log into an application or system account. Using interactive login means there is no accountability or traceability of actions taken by that individual.
IPS	Acronym for "intrusion prevention system."
ISO	Acronym for "International Organization for Standardization."
Issuer	Also referred to as "issuing bank" or "issuing financial institution." Entity that issues payment cards or performs, facilitates, or supports issuing services, including but not limited to issuing banks and issuing processors.
Issuing services	Examples of issuing services include but are not limited to authorization and card personalization.
Keyed Cryptographic Hash	A hashing function that incorporates a randomly generated secret key to provide brute force attack resistance and secret authentication integrity. Appropriate keyed cryptographic hashing algorithms include but are not limited to: HMAC, CMAC, and GMAC, with an effective cryptographic strength of at least 128-bits (*NIST SP 800-131Ar2)*. Refer to the following for more information about HMAC, CMAC, and GMAC, respectively: *NIST SP 800-107r1, NIST SP 800-38B, and NIST SP 800-38D).* See *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms* §5.3.
Key Custodian	A role where a person(s) is entrusted with, and responsible for, performing key management duties involving secret and/or private keys, key shares, or key components on behalf of an entity.
Key Management System	A combination of hardware and software that provides an integrated approach for generating, distributing, and/or managing cryptographic keys for devices and applications.
LAN	Acronym for "local area network."
LDAP	Acronym for "Lightweight Directory Access Protocol."
Least Privileges	The minimum level of privileges necessary to perform the roles and responsibilities of the job function.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Legal Exception	A legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement. Contractual obligations or legal advice are **not** legal restrictions. See the following PCI DSS v4.x documents for information on reporting legal exceptions: • *The Report on Compliance (ROC) Template* and related *Attestations of Compliance*. • *The Self-Assessment Questionnaires (SAQs)* and related *Attestations of Compliance*. *Note: Where an entity operates in multiple locations, a legal exception may only be claimed for the locations governed by the law, regulation, or regulatory requirement, and may not be claimed for locations in which such law, regulation, or regulatory requirement is inapplicable.*
Log	See *Audit Log*.
Logical Access Control	Mechanisms that limit the availability of information or information-processing resources only to authorized persons or applications. See *Physical Access Control*.
MAC	In cryptography, an acronym for "message authentication code." See *Strong Cryptography*.
Magnetic-Stripe Data	See *Track Data*.
Masking	Method of concealing a segment of PAN when displayed or printed. Masking is used when there is no business need to view the entire PAN. Masking relates to protection of PAN when displayed on screens, paper receipts, printouts, etc. See *Truncation* for protection of PAN when electronically stored, processed, or transmitted.
Media	Physical material, including but not limited to, electronic storage devices, removable electronic media, and paper reports.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services. A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
MO/TO	Acronym for "Mail-Order/Telephone-Order."
Multi-Factor Authentication	Method of authenticating a user whereby at least two factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints and other biometric elements).

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Multi-Tenant Service Provider	A type of Third-Party Service Provider that offers various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or "shopping cart" services, web-based hosting services, payment applications, various cloud applications and services, and connections to payment gateways and processors. See *Service Provider* and *Third-Party Service Provider*.
NAC	Acronym for "Network Access Control."
NAT	Acronym for "Network Address Translation."
Network Connection	A logical, physical, or virtual communication path between devices that allows the transmission and reception of network layer packets.
Network Diagram	A diagram showing system components and connections within a networked environment.
Network Security Controls (NSC)	Firewalls and other network security technologies that act as network policy enforcement points. NSCs typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.
NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.
Non-Console Access	Logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external or remote networks.
NTP	Acronym for "Network Time Protocol."
Organizational Independence	An organizational structure that ensures there is no conflict of interest between the person or department performing the activity and the person or department assessing the activity. For example, individuals performing assessments are organizationally separate from the management of the environment being assessed.
OWASP	Acronym for "Open Web Application Security Project."
PAN	Acronym for "primary account number." Unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer and the cardholder account.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Password / Passphrase	A string of characters that serve as an authentication factor for a user or account.
Patch	Update to existing software to add function or to correct a defect.
Participating Payment Brand	Also referred to as "payment brand." A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of writing, Participating Payment Brands include PCI SSC Founding Members and Strategic Members.
Payment Brand	An organization with branded payment cards or other payment card form factors. Payment brands regulate where and how the payment cards or other form factors carrying its brand or logo are used. A payment brand may be a PCI SSC Participating Payment Brand or other global or regional payment brand, scheme, or network.
Payment Card Form Factor	Includes physical payment cards as well as devices with functionality that emulates a payment card to initiate a payment transaction. Examples of such devices include, but are not limited to, smartphones, smartwatches, fitness bands, key tags, and wearables such as jewelry.
Payment Cards	For purposes of PCI DSS, any payment card form factor that bears the logo of any PCI SSC Participating Payment Brand.
Payment Channel	Methods used by merchants to accept payments from customers. Common payment channels include card present (in person) and card not present (e-commerce and MO/TO).
Payment Page	A web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data, for purposes of processing and authorizing payment transactions. The payment page can be rendered as any one of: • A single document or instance, • A document or component displayed in an inline frame within a non-payment page, • Multiple documents or components each containing one or more form elements contained in multiple inline frames within a non-payment page.
Payment Page Scripts	Any programming language commands or instructions on a payment page that are processed and/or interpreted by a consumer's browser, including commands or instructions that interact with a page's document object model. Examples of programming languages are JavaScript and VB script; neither markup-languages (for example, HTML) or style-rules (for example, CSS) are programming languages.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Payment Processor	Sometimes referred to as “payment gateway” or “payment service provider (PSP).” Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. See *Acquirers*.
PCI DSS	Acronym for “Payment Card Industry Data Security Standard.”
Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of cardholder data and/or sensitive authentication data. See *Visitor.*
Phishing Resistant Authentication	Authentication designed to prevent the disclosure and use of authentication secrets to any party that is not the legitimate system to which the user is attempting to authenticate (for example, through in-the-middle (ITM) or impersonation attacks). Phishing-resistant systems often implement asymmetric cryptography as a core security control. Systems that rely solely on knowledge-based or time-limited factors such as passwords or one-time-passwords (OTPs) are not considered phishing resistant, nor are SMS or magic links. Examples of phishing-resistant authentication includes FIDO2.
Physical Access Control	Mechanisms that limit the access to a physical space or environment to only authorized persons. See *Logical Access Control*.
PIN	Acronym for “personal identification number.”
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain the PAN (or a truncation thereof) depending on the approved ISO PIN Block Format used.
POI	Acronym for “Point of Interaction,” the initial point where data is read from a card.
Point of Sale System (POS)	Hardware and software used by merchants to accept payments from customers. May include POI devices, PIN pads, electronic cash registers, etc.
Privileged User	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.
QIR	Acronym for “Qualified Integrator or Reseller.” Refer to the *QIR Program Guide* on the PCI SSC website for more information.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
QSA	Acronym for "Qualified Security Assessor." QSA companies are qualified by PCI SSC to validate an entity's adherence to PCI DSS requirements. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees.
Remote Access	Access to an entity's network from a location outside of that network. An example of technology for remote access is a VPN.
Removable Electronic Media	Media that stores digitized data that can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives, and external/portable hard drives. In this context, removable electronic media does not include hot-swappable drives, tape drives used for bulk back-ups, or other media not typically used to transport data from one location for use in another.
Risk Assessment	Enterprise-wide process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure. See *Targeted Risk Analysis*.
Risk Ranking	Process of classifying risks to identify, prioritize, and address items in the order of importance.
ROC	Acronym for "Report on Compliance." Reporting tool used to document detailed results from an entity's PCI DSS assessment.
RSA	Algorithm for public-key encryption. See *Strong Cryptography*.
SAQ	Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. See PCI DSS section: *4 Scope of PCI DSS Requirements*.
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.
Security Event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.
Security Officer	Primary person responsible for an entity's security.
Segmentation	Also referred to as "network segmentation" or "isolation." Segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. See "Segmentation" in PCI DSS section: *4 Scope of PCI DSS Requirements*.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Sensitive Area	A sensitive area is typically a subset of the CDE and is any area that houses systems considered critical to the CDE. This includes data centers, server rooms, back-office rooms at retail locations, and any area that concentrates or aggregates cardholder data storage, processing, or transmission. Sensitive areas also include areas housing systems that manage or maintain the security of the CDE (for example, those providing network security controls or that manage physical or logical security). This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store or call centers where agents are taking payments.
Sensitive Authentication Data (SAD)	Security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.
Separation of Duties	Practice of dividing steps in a function among multiple individuals, to prevent a single individual from subverting the process.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things, such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data (CHD) and/or sensitive authentication data (SAD) on behalf of another entity. This includes payment gateways, payment service providers (PSPs), and independent sales organizations (ISOs). This also includes companies that provide services that control or could impact the security of CHD and/or SAD. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities. If an entity provides a service that involves *only* the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services). See *Multi-Tenant Service Provider* and *Third-Party Service Provider.*
SNMP	Acronym for “Simple Network Management Protocol.”.
Split Knowledge	A method by which two or more entities separately have key components or key shares that individually convey no knowledge of the resultant cryptographic key.
SQL	Acronym for “Structured Query Language.”
SSH	Abbreviation for “Secure Shell.”
SSL	Acronym for “Secure Sockets Layer.”

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Strong Cryptography	Cryptography is a method to protect data through a reversible encryption process, and is a foundational primitive used in many security protocols and services. Strong cryptography is based on industry-tested and accepted algorithms along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Effective key strength can be shorter than the actual 'bit' length of the key, which can lead to algorithms with larger keys providing lesser protection than algorithms with smaller actual, but larger effective, key sizes. *It is recommended that all new implementations use a minimum of 128-bits of effective key strength.* Examples of industry references on cryptographic algorithms and key lengths include: • *NIST Special Publication 800-57 Part 1,* • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018), and* • *ISO/IEC 18033 Encryption algorithms, and* • *ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.*
System Components	Any network devices, servers, computing devices, virtual components, or software included in or connected to the CDE, or that could impact the security of cardholder data and/or sensitive authentication data.
System-level object	Anything on a system component that is required for its operation, including but not limited to application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.
Targeted Risk Analysis	For PCI DSS purposes, a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement.
TDES	Acronym for "Triple Data Encryption Standard." Also referred to as "3DES" or "Triple DES."
Telnet	Abbreviation for "telephone network protocol."
Third-Party Service Provider (TPSP)	Any third party acting as a service provider on behalf of an entity. See *Multi-Tenant Service Provider* and *Service Provider*.
Third-Party Software	Software that is acquired by, but not developed expressly for, an entity. It may be open source, freeware, shareware, or purchased.
TLS	Acronym for "Transport Layer Security."

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

Term	Definition
Token	In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or multi-factor authentication.
Track Data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the track data on the magnetic stripe.
Truncation	Method of rendering a full PAN unreadable by removing a segment of PAN data. Truncation relates to protection of PAN when electronically stored, processed, or transmitted. See *Masking* for protection of PAN when displayed on screens, paper receipts, etc.
Trusted Network	Network of an entity that is within the entity's ability to control or manage and that meets applicable PCI DSS requirements.
Untrusted Network	Any network that does not meet the definition of a "trusted network."
Virtual Payment Terminal	In the context of Self-Assessment Questionnaire (SAQ) C-VT, a virtual payment terminal is web-browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data through a web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtualization	The logical abstraction of computing resources from physical and/or logical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. Other common abstractions include, but are not limited to, containers, serverless computing, or microservices.
Visitor	A vendor, guest of any personnel, service worker, or personnel that normally do not have access to the subject area. Cardholders present in a retail location to purchase goods or services are not considered "visitors." See *Cardholder* and *Personnel.*
VPN	Acronym for "virtual private network."
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
Web Application	An application that is generally accessed through a web browser or through web services. Web applications may be available through the Internet or a private, internal network.

© 2006 - 2024 PCI Security Standards Council, LLC. All rights reserved.

UNITED STATES DEPARTMENT OF EDUCATION

STUDENT PRIVACY POLICY OFFICE

SPPO-21-01

Protection of Pupil Rights Amendment (PPRA)

Other than statutory and regulatory requirements included in the document, the contents of this guidance do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

Rights of Parents under PPRA

PPRA (20 U.S.C. § 1232h, 34 CFR Part 98) affords parents of students certain rights regarding, among other things, participation in surveys, the collection and use of information for marketing purposes, and certain physical exams. These include, but are not limited to, the right to:

- *Consent* before students are required to submit to a survey that concerns one or more of the following eight protected areas (protected information survey) if the survey is funded as part of a program administered by the U.S. Department of Education (Department) (applicable program) –

  1. Political affiliations or beliefs of the student or student's parent;
  2. Mental or psychological problems of the student or student's family;
  3. Sex behavior or attitudes;
  4. Illegal, anti-social, self-incriminating, or demeaning behavior;
  5. Critical appraisals of others with whom respondents have close family relationships;
  6. Legally recognized privileged or analogous relationships, such as with lawyers, doctors, or ministers;
  7. Religious practices, affiliations, or beliefs of the student or student's parent; or
  8. Income, other than as required by law to determine program eligibility.

- *Receive notice* and an opportunity to *opt a student out* of –

  1. Any protected information survey administered or distributed to a student by an local educational agency that is a recipient of funds under an applicable program (LEA) if the protected information survey is either not funded as part of a program administered by the Department or is funded as part of a program administered by the Department but to which a student is not required to submit;
  2. Any non-emergency, invasive physical examination or screening required by an LEA as a condition of attendance; administered by the school and scheduled by the school in advance; and, that is not necessary to protect the immediate health and safety of a student, with some exceptions; and
  3. Activities of an LEA involving collection, disclosure, or use of personal information collected from students for the purpose of marketing or sale (or to otherwise distribute such information to others for that purpose), with some exceptions.

Issued October 22, 2020

- *Inspect*, upon request –

    1. Protected information surveys and surveys created by a third party, before the administration or distribution by an LEA of the surveys to a student;

    2. Any instrument used by an LEA to collect personal information for the purpose of marketing or sale (or otherwise distributing such information for that purpose), before the instrument is administered or distributed to a student, with some exceptions; and

    3. Instructional material, excluding academic tests or academic assessments, used by an LEA as part of the educational curriculum for a student.

These rights transfer from the parents to the student when the student turns 18 years old or becomes an emancipated minor under applicable State law.

Requirements of LEAs under PPRA

LEAs are required to develop and adopt policies, in consultation with parents, to address the protection of student privacy and parents' rights under PPRA, including those discussed above. In addition, LEAs must directly notify parents of these policies at least annually, at the start of each school year, and within a reasonable period after any substantive change to the policies.

LEAs must also directly notify, such as through U.S. Mail or email, parents of students who are scheduled or expected to be scheduled to participate in any of the activities or surveys listed below and must provide an opportunity for parents to opt their child out of participation. LEAs must make this notification to parents at least annually at the beginning of the school year, and this notification must include the specific or approximate dates when the activities or surveys are scheduled or expected to be scheduled. For activities or surveys that are scheduled after the school year starts, LEAs must provide parents with reasonable notification and an opportunity to review, as well as an opportunity to opt their child out. These activities and surveys involve:

- Collection, disclosure, or use of personal information collected from students for the purpose of marketing or sale (or otherwise distributing such information to others for that purpose), with some exceptions;

- Administration or distribution to a student of any protected information survey not funded as part of a program administered by the Department or funded as part of a program administered by the Department but to which students are not required to submit; and

- Certain non-emergency, invasive physical examinations or screenings, as described above.

Parents who seek additional resources on student privacy under PPRA may visit the Department's Student Privacy Policy Office website at https://studentprivacy.ed.gov/. Parents who believe their PPRA rights have been violated may file a complaint online by selecting the PPRA complaint form option at https://studentprivacy.ed.gov/file-a-complaint or by mailing the form to the following address:

Student Privacy Policy Office
U.S. Department of Education
400 Maryland Avenue, S.W.
Washington, D.C. 20202

HB166

W11V3EE-2

By Representatives Hulsey, Collins, Baker, Faulkner, DuBose

RFD: Education Policy

First Read: 04-Feb-25

A BILL

TO BE ENTITLED

AN ACT

Relating to public K-12 education; to establish the Freeing our Classrooms of Unnecessary Screens for Safety (FOCUS) Act; to prohibit the use, operation, and possession of wireless communication devices on certain public school properties; to require local boards of education to adopt an Internet safety policy; to add Section 16-40-13 to the Code of Alabama 1975, to require students to complete a social media safety course prior to entering the eighth grade; and to repeal Section 16-1-27, Code of Alabama 1975, providing for the use of electronic communication devices on school property.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. The Legislature finds and declares the following:

(1) Each student in an Alabama public K-12 school should be college-ready or career-ready upon high school graduation.

(2) Many high school teachers believe that cell phones and other electronic communication devices are distracting students in the classroom.

(3) Studies have shown that cell phones and other electronic communication devices are negatively impacting learning outcomes.

(4) Studies have shown that increased social media usage may negatively affect the mental health of school-aged children.

Section 2. For the purposes of this act, the following terms have the following meanings:

(1) INSTRUCTIONAL DAY. The period of time during which a public elementary or secondary school is open and in session for purpose of meeting the minimum number of instructional days or hours pursuant to Section 16-13-231, Code of Alabama 1975. The term also includes class transitions, lunch, non-instructional times, and any other time specified in a wireless communication device policy.

(2) WIRELESS COMMUNICATION DEVICE. A cellular telephone, tablet computer, laptop computer, pager, gaming device, or any other portable electronic device identified in a wireless communication device policy that has the capability of exchanging voice, messaging, or other data communication with another electronic device.

(3) WIRELESS COMMUNICATION DEVICE POLICY. A written policy adopted by a local board of education to implement this act.

Section 3. (a) Beginning with the 2025-2026 school year, no student shall use or operate any wireless communication device in any public elementary or secondary school building or on the grounds thereof during the instructional day.

(b) Beginning with the 2025-2026 school year, no student may possess a wireless communication device in any public elementary or secondary school building or on the grounds thereof during the instructional day unless the wireless communication device is turned off and stored off their person in a locker, car, or similar storage location.

(c) Notwithstanding subsections (a) and (b), a student may use, operate, or possess a wireless communication device in a public elementary or secondary school building or on the grounds thereof during the instructional day in any of the following circumstances:

(1) The use, operation, or possession is pursuant to the student's Individualized Education Program, Individualized Accommodation Plan, Section 504 plan, or Individualized Health Plan.

(2) The use, operation, or possession is for educational or learning purposes under the supervision of local board of education personnel.

(3) The use, operation, or possession occurs during an emergency threatening the life or safety of the student or another person.

(d) No later than July 1, 2025, each local board of education shall adopt a wireless communication device policy. The wireless communication device policy shall include

consequences for violations. The local board of education shall reasonably distribute the wireless communication device policy to students, parents, faculty, staff, and the State Board of Education.

Section 4. (a) No later than July 1, 2025, each local board of education shall adopt an Internet safety policy that addresses student access to the Internet on devices owned by the local board of education.

(b) The policy shall do all of the following:

(1) Limit Internet access by students to only age-appropriate subject matters and materials deemed age-appropriate pursuant to the policy.

(2) Provide specific procedures and other protections that prioritize the safety and security of students when using email, chat rooms, and other forms of direct electronic communication.

(3) Prohibit access by students to unlawfully obtained data or information, including hacking, and other unlawful online activity by students.

(4) Prohibit access to websites, web applications, or software that exposes students to the disclosure, use, or dissemination of their personal information.

(5) Prohibit students from accessing social media platforms, except when expressly directed by a teacher solely for educational purposes.

(c) The principal shall be responsible for ensuring consistent compliance with the policy by school personnel.

Section 5. (a) Each certificated staff member employed by the local board education shall complete an annual written anonymous survey regarding the implementation of the wireless communication device policy and to measure uniform compliance within the school.

(b) On or before October 1, 2025, the State Department of Education shall develop a survey to assess the levels of participation and compliance with the wireless communication device policy. On or before June 1, each subsequent year, the annual survey results shall be submitted by the principal to the local superintendent of education, local board of education, and the State Board of Education for publication on the website of the State Department of Education.

Section 6. Section 16-40-13 is added to the Code of Alabama to read as follows:

§16-40-13

(a) No later than July 1, 2025, the State Department of Education shall develop and approve an asynchronous, digitally delivered course that addresses the risks of using social media and how to use social media safely.

(b) At a minimum, the course shall include the following topics:

(1) The benefits of safely using age-appropriate social media platforms, including career and resume building for future academic or employment opportunities; sharing information with family and friends; and safely connecting with other users with similar interests.

(2) The risks of social media use including its negative effects on mental health, including addiction; the distribution of misinformation on social media; how social media manipulates behavior; and the permanency of sharing materials online.

(3) Safe practices for using social media including how to report suspicious behavior; how to identify cyberbullying, phishing and scam communications, predatory behavior, and human trafficking; and maintaining personal security and preventing oversharing of personal information.

(c) The State Department of Education shall make the course available online and each local board of education shall reasonably notify parents of its availability. Each local board of education shall deliver the course to all students prior to entering the eighth grade and shall make the course available to students in grades eight through 12 who transfer to the school district or who otherwise have not completed the course.

(d) The State Board of Education may adopt rules to implement this section.

Section 7. Section 16-1-27, Code of Alabama 1975, providing for the use of electronic communications devices on school property, is repealed.

Section 8. This act shall become effective immediately.

House of Representatives

Read for the first time and referred 04-Feb-25
to the House of Representatives
committee on Education Policy

Read for the second time and placed 27-Feb-25
on the calendar:
0 amendments

Read for the third time and passed 03-Apr-25
as amended
Yeas 79
Nays 15
Abstains 9

John Treadwell
Clerk

SB318

192523-5

By Senators Orr and Holley

RFD: Governmental Affairs

First Read: 13-FEB-18

ACT #2018-396



SB318

ENROLLED, An Act,

Relating to consumer protection; to require certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act may be cited and shall be known as the Alabama Data Breach Notification Act of 2018.

Section 2. For the purposes of this act, the following terms have the following meanings:

(1) BREACH OF SECURITY or BREACH. The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does not include any of the following:

a. Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.

b. The release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

c. Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

(2) COVERED ENTITY. A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.

(3) DATA IN ELECTRONIC FORM. Any data stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices.

(4) GOVERNMENT ENTITY. The State, a county, or a municipality or any instrumentality of the state, a county, or a municipality.

(5) INDIVIDUAL. Any Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.

(6) SENSITIVE PERSONALLY IDENTIFYING INFORMATION.

a. Except as provided in paragraph b., an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident:

1. A non-truncated Social Security number or tax identification number.

2. A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.

3. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.

4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

b. The term does not include either of the following:

1. Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media.

2. Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.

(7) THIRD-PARTY AGENT. An entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity.

Section 3. (a) Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security.

(b) Reasonable security measures means security measures practicable for the covered entity subject to

subsection (c), to implement and maintain, including consideration of all of the following:

(1) Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security. An owner or manager may designate himself or herself.

(2) Identification of internal and external risks of a breach of security.

(3) Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards.

(4) Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.

(5) Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information.

(6) Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures; provided, however, that the management of a government entity subject to this subdivision may be appropriately informed of the status of its security measures through a properly convened execution session under the Open Meetings Act pursuant to Section 36-25A-7, Code of Alabama 1975.

(c) An assessment of a covered entity's security shall be based upon the entity's reasonable security measures as a whole and shall place an emphasis on data security failures that are multiple or systemic, including consideration of all the following:

(1) The size of the covered entity.

(2) The amount of sensitive personally identifying information and the type of activities for which the sensitive personally identifying information is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity.

(3) The covered entity's cost to implement and maintain the reasonable security measures to protect against a breach of security relative to its resources.

Section 4. (a) If a covered entity determines that a breach of security has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity, the covered entity shall conduct a good faith and prompt investigation that includes all of the following:

(1) An assessment of the nature and scope of the breach.

(2) Identification of any sensitive personally identifying information that may have been involved in the

breach and the identity of any individuals to whom that information relates.

(3) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(4) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.

(b) In determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization, the following factors may be considered:

(1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information.

(2) Indications that the information has been downloaded or copied.

(3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(4) Whether the information has been made public.

Section 5. (a) A covered entity that is not a third-party agent that determines under Section 4 that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, shall give notice of the breach to each individual.

(b) Notice to individuals under subsection (a) shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation in accordance with Section 4. Except as provided in subsection (c), the covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(c) If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the receipt of written request of the law enforcement agency for a period that the law enforcement agency determines is

necessary. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request made under this section if further delay is necessary.

(d) Except as provided by subsection (e), notice to an affected individual under this section shall be given in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the email address of the individual in the records of the covered entity. The notice shall include, at a minimum, all of the following:

(1) The date, estimated date, or estimated date range of the breach.

(2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.

(3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.

(4) A general description of steps an affected individual can take to protect himself or herself from identity theft.

(5) Information that the individual can use to contact the covered entity to inquire about the breach.

(e)(1) A covered entity required to provide notice to any individual under this section may provide substitute notice in lieu of direct notice, if direct notice is not feasible due to any of the following:

a. Excessive cost. The term includes either of the following:

1. Excessive cost to the covered entity relative to the resources of the covered entity.

2. The cost to the covered entity exceeds five hundred thousand dollars ($500,000).

b. Lack of sufficient contact information for the individual required to be notified.

c. The affected individuals exceed 100,000 persons.

(2) a. Substitute notice shall include both of the following:

1. A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days.

2. Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

b. An alternative form of substitute notice may be used with the approval of the Attorney General.

(f) If a covered entity determines that notice is not required under this section, the entity shall document the

determination in writing and maintain records concerning the determination for no less than five years.

Section 6. (a) If the number of individuals a covered entity is required to notify under Section 5 exceeds 1,000, the entity shall provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay. Except as provided in subsection (c) of Section 5, the covered entity shall provide the notice within 45 days of the covered entity's receipt of notice from a third party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(b) Written notice to the Attorney General shall include all of the following:

(1) A synopsis of the events surrounding the breach at the time that notice is provided.

(2) The approximate number of individuals in the state who were affected by the breach.

(3) Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services.

(4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

(c) A covered entity may provide the Attorney General with supplemental or updated information regarding a breach at any time.

(d) Information marked as confidential that is obtained by the Attorney General under this section is not subject to any open records, freedom of information, or other public record disclosure law.

Section 7. If a covered entity discovers circumstances requiring notice under Section 5 of more than 1,000 individuals at a single time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. 1681a, of the timing, distribution, and content of the notices.

Section 8. In the event a third-party agent has experienced a breach of security in the system maintained by the agent, the agent shall notify the covered entity of the breach of security as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. After receiving notice from a third-party

agent, a covered entity shall provide notices required under Sections 5 and 6. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements. A covered entity may enter into a contractual agreement with a third-party agent whereby the third-party agent agrees to handle notifications required under this act.

Section 9. (a) A violation of the notification provisions of this act is an unlawful trade practice under the Alabama Deceptive Trade Practices Act, Chapter 19, Title 8, Code of Alabama 1975, but does not constitute a criminal offense under Section 8-19-12, Code of Alabama 1975. The Attorney General shall have the exclusive authority to bring an action for civil penalties under this act.

(1) A violation of this act does not establish a private cause of action under Section 8-19-10, Code of Alabama 1975. Nothing in this act may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise.

(2) Any covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this act will be subject to the penalty provisions set out in Section 8-19-11, Code of Alabama 1975. For the purposes of this act, knowingly shall

mean willfully or with reckless disregard in failing to comply with the notice requirements of Sections 5 and 6. Civil penalties assessed under Section 8-19-11, Code of Alabama 1975, shall not exceed five hundred thousand dollars ($500,000) per breach.

(b)(1) Notwithstanding any remedy available under subdivision (2) of subsection (a) of this section, a covered entity that violates the notification provisions of this act shall be liable for a civil penalty of not more than five thousand dollars ($5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this act.

(2) The office of the Attorney General shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named individual or individuals. In such an action brought by the office of the Attorney General, recovery shall be limited to actual damages suffered by the person or persons, plus reasonable attorney's fees and costs.

(3) It is not a violation of this act to refrain from providing any notice required under this act if a court of competent jurisdiction has directed otherwise.

(4) To the extent that notification is required under this act as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of

the breach shall subject the third-party agent to the fines and penalties set forth in the act.

(5) Government entities shall be subject to the notice requirements of this act. A government entity that acquires and maintains sensitive personally identifying information from a government employer, and which is required to provide notice to any individual under this act, must also notify the employing government entity of any individual to whom the information relates.

(6) All government entities are exempt from any civil penalty authorized by this act; provided, however, the Attorney General may bring an action against any state, county, or municipal official or employee, in his or her official capacity, who is subject to this act for any of the following:

a. To compel the performance of his or her duties under this act.

b. To compel the performance of his or her ministerial acts under this act.

c. To enjoin him or her from acting in bad faith, fraudulently, beyond his or her authority, or under mistaken interpretation of the law.

(7) By February 1 of each year, the Attorney General shall submit a report to the Governor, the President Pro Tempore of the Senate, and the Speaker of the House of

Representatives describing the nature of any reported breaches of security by government entities or third-party agents of government entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any government entity that has violated any of the applicable requirements in this act in the preceding calendar year.

Section 10. A covered entity or third-party agent shall take reasonable measures to dispose, or arrange for the disposal, of records containing sensitive personally identifying information within its custody or control when the records are no longer to be retained pursuant to applicable law, regulations, or business needs. Disposal shall include shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.

Section 11. An entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal government is exempt from this act as long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to affected individuals pursuant to those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Section 12. An entity subject to or regulated by state laws, rules, regulations, procedures, or guidance on data breach notification that are established or enforced by state government, and are at least as thorough as the notice requirements provided by this act, is exempt from this act so long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to affected individuals pursuant to the notice requirements of those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Section 13. This act shall become effective on the first day of the third month following its passage and approval by the Governor, or its otherwise becoming law.

President and Presiding Officer of the Senate

Speaker of the House of Representatives

SB318

Senate 01-MAR-18

I hereby certify that the within Act originated in and passed the Senate, as amended.

Patrick Harris,
Secretary.

House of Representatives
Amended and passed 22-MAR-18

Senate concurred in House amendment 27-MAR-18

APPROVED 3-28-2018

By: Senator Orr **TIME** 3:37 PM

GOVERNOR

Alabama Secretary Of State

Act Num....: 2018-396
Bill Num...: S-318

Recv'd 03/28/18 04:21pmSLF

HOUSE ACTION
(Continued)

HOUSE OF REPRESENTATIVES
R. 3 at length and passed
Yeas 101 Nays 0 Abs 0
Date 3-22-18
as amended
JEFF WIGGINS, Clerk