A close-up of a computer chip

Description automatically generated with low confidence

Ohio Cyber Collaboration Committee

Adjutant General’s Department

Office: 614-336-4903

# [ ]

# Incident Response Guide

# Based on the NIST Cybersecurity Framework

2022-2023

This document is confidential and contains PII as well as operational incident response processes.

Table of Contents

|  |  |  |
| --- | --- | --- |
| **Introduction** | **Description** | **Page** |
| SECTION 1 | Glossary and Acronyms |  |
| 1.1 | Glossary | 6 |
|  | Common Acronyms | 13 |
| SECTION 2 | Security Incident Response Procedure | 14 |
| SECTION 3 | Privacy/Security Event Initial Triage Checklist | 22 |
| SECTION 4 | Event Threat, Impact Analysis, and Escalation Criteria | 23 |
| 4.1 | Event Threat and Impact Analysis | 23 |
| 4.2 | Event Escalation: Communication | 23 |
| SECTION 5 | Breach Notice Criteria | 24 |
| 5.1 | Ohio Legal Requirements for Breach Notices | 24 |
| 5.2 | Federal Legal Requirements for Breach Notices | 30 |
| 5.3 | Security Breach Notification Statute in Ohio | 31 |
| SECTION 6 | Post-Incident Checklist | 33 |
| SECTION 7 | Incident Response Team Templates | 34 |
| 7.1 | Title and Contact Information for Plan Sponsor/Owner | 34 |
| 7.2 | IRT Charter | 34 |
| 7.3 | IRT Membership by Roles | 35 |
| 7.4 | Supply Chain Membership and Roles | 35 |
| 7.5 | IRT Meeting Minutes | 36 |
| 7.6 | IRT Action List | 37 |
| 7.7 | IRT State Government Contact Information | 38 |
| SECTION 8 | Additional Templates | 39 |
| 8.1 | Identity Theft Protection Criteria | 39 |
| 8.2 | Internal Management Alert Template | 40 |
| 8.3 | Notice to Individuals Affected by Incident | 41 |
| 8.4 | Public (Media) Notice | 43 |
| 8.5 | Post-Mortem and Improvement Plan | 44 |
| SECTION 9 | External Contacts | 45 |
| 9.1 | State of Ohio Contacts | 45 |
| 9.2 | Federal Contacts | 48 |
| 9.3 | Industry Contacts | 49 |
| 9.4 | Press Contacts | 50 |
| SECTION 10 | Legal References | 50 |
| 10.1 | Ohio Laws and Regulations for Data Privacy and Security | 51 |
| 10.2 | Federal Laws and Regulations for Data Privacy and Security | 51 |
| 10.3 | Other Laws and Regulations for Data Privacy and Security | 54 |
|  | Acknowledgements | 54 |

## Introduction

When a privacy or information security incident occurs, it is imperative that [Name of Organization] follow documented procedures for responding to and processing the incident. An Incident Response Plan (IRP) is intended to contain the procedures and plans for such incidents when they occur. This plan should be in both hard copy and electronic formats and be readily available to any standing member of the IR team.

Two principles guide the establishment of the IRP. First, is that [Name of Organization] must establish in advance and maintain a plan for responding to an incident. Second, [Name of Organization] must test and update the operation of the plan periodically to ensure that it is appropriate and functional.

This Incident Response Team (the “IRT”) Charter establishes membership, subject matter experts, roles, responsibilities, and activities of the [Name of Organization] IRT to respond to an actual or suspected information privacy or security event/incident.

### Contact Information for Plan Sponsor/Owner

### For questions or further information, please contact:

### [Insert Appropriate Name and Title]

[Insert Address]

**IRT Mission:**

The IRT mission is, first, to prevent incidents by reasonably anticipating, detecting, and planning for actual and suspected privacy or security events; and second, to respond to and mitigate privacy or security events.

**Overview:**

The Incident Response Team (the “IRT”) is a standing team of internal personnel established by the organization in this Guide with expertise in responding to a significant actual or suspected privacy or security event or incident. The IRT operates on behalf of [Name of Organization] and engages, informs, and receives support from [Name of Organization]. There is a set protocol to initiate the IRT activities in response to an actual or suspected event/incident. Once activated, the IRT has authority to establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours.

**Responsibilities and Roles:**

Responsibilities:

1. **Anticipate and prepare** [Name of Organization] for privacy or security events/incidents which can be reasonably anticipated;
2. **Respond** to actual or suspected events/incidents on behalf of [Name of Organization] as needed, with activities such as:
   1. Triage (see section 2);
   2. Communication, internal and external, as needed according to [Name of Organization]’s communications protocol.
   3. Track and document IRT activities and discoveries; and
   4. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

* Uncontained or escalating malware attack on system (computer virus, worm, bot, or Trojan);
* Abuse, theft, misuse, or loss of data or hardware (including unauthorized use, disclosure, or access to computer accounts, systems, or data; hacking; human error);
* Improper use or disclosure of information or information resources as outlined in the organization standards or contracts including e-mail, equipment, Internet, and acceptable data use
  + (includes human resources or contractor misuse or error);
* Many individuals or a large amount of sensitive data impacted; or
* Events likely to be high-profile or create a significant risk of individual harm (e.g., risk of financial harm, reputational harm, or medical identity theft).

Roles:

1. **The IRT Lead.** The Lead of the IRT may:
2. Be designated by and reporting to Chief Technology Officer. The IRT is led by System Administrator/Network Administrator or the CTO designee.
3. Declare an incident
4. Establish, maintain, and update written IRT protocols or incident response plans
5. Identify roles and responsibilities for IRT standing members
6. Request or designate ad hoc members for particular events as needed
7. Request event response priorities which may supersede daily business responsibilities or require attention outside normal business hours
8. **IRT Standing Members.** The standing members include named individuals or representatives.
9. **Ad hoc Members or Subject Matter Experts.** Ad hoc members or Subject Matter Experts may be designated as ad hoc resources by the IRT Lead.

### 

IRT Membership by Roles

The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another organization employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

**Standing IRT Membership Contact Information - *for Incident Response***

***Insert BEFORE\_Incident Response Guide Planning Here- IRT Members by Roles Sheet***

***OR Complete table***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standing Members** | **Name** | **Phone** | **Email** | **After-hours contact** |
| IRT Lead |  |  |  |  |
| [Chief Technology Officer/Technology Director or designee] |  |  |  |  |
| [Network Administrator] |  |  |  |  |
| [Systems Administrator] |  |  |  |  |
| [Technology Administrative Assistant] |  |  |  |  |
| [Technicians] |  |  |  |  |
| [Teaching and Learning Coaches] |  |  |  |  |
| [Data Coordinator] |  |  |  |  |
| [Other] |  |  |  |  |
| Legal Counsel to the IRT – to avoid losing attorney-client  privilege, *do not list legal as a member* |  |  |  |  |

Supply Chain Membership by Roles

The following table contains contact information for current Supply Chain members. Please note that, in some cases, a member listed below may have designated another organization employee to represent him or her.

[Name of Organization]  ***Insert BEFORE\_Incident Response Guide Planning Here- See Supply Chain (Vendor List) Sheet***

**Standing Supply Chain Membership Contact Information**

***Insert BEFORE\_Incident Response Guide Planning Here -See IRT Members By Roles Sheet***

**SECTION 1 - Glossary and Acronyms**

### Glossary

**Access**

From CNSSI 4009: The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

**Access Control**

Adapted From CNSSI 4009: The process of granting or denying specific requests for or attempts to:

1. obtain and use information and related information processing services; and
2. enter specific physical facilities.

**Adversary**

From DHS Risk Lexicon: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

**Air Gap**

To physically separate or isolate a system from other systems or networks (verb). The physical separation or isolation of a system from other systems or networks.

**Asset**

DHS Risk Lexicon: A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value. Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

**Attack**

From NCSD Glossary. NTSSI 4009 (2000), CNSSI 4009: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. The intentional act of attempting to bypass one or more security services or controls of an information system.

**Attack Surface**

The set of ways in which an adversary can enter a system and potentially cause damage. An information system's characteristics that permit an adversary to probe, attack, or maintain presence in the information system.

**Authentication**

Adapted From CNSSI 4009, NIST SP 800-21, NISTIR 7298: The process of verifying the identity or other attributes of an entity (user, process, or device). Also the process of verifying the source and integrity of data.

**Breach**

Ohio: Unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

**Cloud Computing**

Adapted from CNSSI 4009, NIST SP 800-145: A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Critical Infrastructure**

Adapted from the National Infrastructure Protection Plan: The systems and assets, whether physical or virtual, are so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

**Cyber Exercise**

Adapted from NCSD Glossary, DHS Homeland Security Exercise and Evaluation Program: A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to, or recovering from the disruption.

**Cybersecurity**

Adapted from CNSSI 4009, NIST SP 800-53 Rev 5: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

**Data Breach**

The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

**Data Loss Prevention**

A set of procedures and mechanisms to stop sensitive data from leaving a security boundary.

**Decode**

From CNSSI 4009: To convert encoded text to plain text by means of a code.

**Decrypt**

From CNSSI 4009: A generic term encompassing decode and decipher.

**Decryption**

Adapted From ICAM SAML 2.0 WB SSO Profile 1.0.2: The process of transforming ciphertext into its original plaintext. The process of converting encrypted data back into its original form, so it can be understood.

**Digital Forensics**

Adapted From CNSSI 4009; NICE Framework: The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes. In the NICE Framework, cybersecurity work where a person: Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability, mitigation, and/or criminal, fraud, counterintelligence, or law enforcement investigations.

**Encrypt**

From CNSSI 4009: The generic term encompassing enciphers and encode.

**Encryption**

Adapted From CNSSI 4009, ICAM SAML 2.0 WB SSO Profile 1.0.2: The process of transforming plaintext into ciphertext. Converting data into a form that cannot be easily understood by unauthorized people.

**Enterprise Risk Management**

Adapted From DHS Risk Lexicon, CNSSI 4009: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization’s ability to achieve its objectives. Involves identifying mission dependencies on enterprise capabilities, identifying and prioritizing risks due to defined threats, implementing countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and assessing enterprise performance against threats and adjusts countermeasures as necessary.

**Event**

Adapted From CNSSI 4009: An observable occurrence in an information system or network. Sometimes provides an indication that an incident is occurring or at least raises the suspicion that an incident may be occurring.

**Exposure**

Adapted From NCSD glossary: The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

**Firewall**

Adapted From CNSSI 4009: A capability to limit network traffic between networks and/or information systems. A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

**Hacker**

From CNSSI 4009: An unauthorized user who attempts to or gains access to an information system.

**ICT supply chain threat**

From DHS SCRM PMO: A man-made threat achieved through exploitation of the information and communications technology (ICT) system’s supply chain, including acquisition processes.  
Related Term(s): supply chain, threat

**Incident**

Adapted From CNSSI 4009, FIPS 200, NIST SP 800-53 Rev 5, ISSG: An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Incident Management**

Adapted From NCSD Glossary, ISSG NCPS Target Architecture Glossary: The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems.

**Incident Response**

In the Workforce framework, cybersecurity work where a person responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

**Incident Response Plan**

Adapted From CNSSI 4009: A set of predetermined and documented procedures to detect and respond to a cyber incident.

**Industrial Control System (ICS)**

Adapted From NIST SP 800-53 Rev 5, NIST SP 800-82: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

**Information Security Policy**

From CNSSI 4009; NIST SP 800-53 Rev 5: An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

**Information Sharing**

Adapted From NCSD glossary: An exchange of data, information, and/or knowledge to manage risks or respond to incidents.

**Information System Resilience**

Adapted From NIST SP 800-53 Rev 5: The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

**Information Technology**

Adapted From CNSSI 4009, NIST SP 800-53 rev. 5, based on 40 U.S.C. sec. 1401: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

**Insider Threat**

Adapted From CNSSI 4009; From NIAC Final Report and Recommendations on the Insider Threat to Critical Infrastructure, 2008: A person or group of persons within an organization who pose a potential risk through violating security policies. One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

**Integrated Risk Management**

Adapted From DHS Risk Lexicon: The structured approach that enables an enterprise or organization to share risk information and risk analysis and to synchronize independent yet complementary risk management strategies to unify efforts across the enterprise.

**Intrusion Detection**

Adapted From CNSSI 4009, ISO/IEC 27039 (draft): The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

**Investigation**

Adapted From ISSG V1.2 Database; Conrad, E., Misenauer, S., & Feldman, J. (2010). CISSP® Study Guide. Burlington, MA: Syngress; From NICE Workforce Framework: A systematic and formal inquiry into a qualified threat or incident using digital forensics and perhaps other traditional criminal inquiry techniques to determine the events that transpired and to collect evidence. In the NICE Framework, cybersecurity work where a person: Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

**Key**

From CNSSI 4009: The numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

**Knowledge Management**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

**Machine Learning and Evolution**

Adapted From DHS personnel: A field concerned with designing and developing artificial intelligence algorithms for automated knowledge discovery and innovation by information systems.

**Malicious Code**

Adapted From CNSSI 4009. NIST SP 800-53 Rev 5: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Includes software, firmware, and scripts.

**Malware**

Adapted From CNSSI 4009, NIST SP 800-83: Software that compromises the operation of a system by performing an unauthorized function or process.

**Network Services**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

**Password**

From FIPS 140-2: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

**Penetration (Pen) Test**

A colloquial term for penetration test or penetration testing.

**Penetration Testing**

Adapted From NCSD Glossary, CNSSI 4009, NIST SP 800-53 Rev 5: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

**Personal Identifying Information / Personally Identifiable Information**

Adapted From NCSD Glossary, CNSSI 4009, GAO Report 08-356, as cited in NIST SP 800-63 Rev 1: The information that permits the identity of an individual to be directly or indirectly inferred.

**Phishing**

Adapted From NCSD Glossary, CNSSI 4009, NIST SP 800-63 Rev 1: A digital form of social engineering to deceive individuals into providing sensitive information.

**Recovery**

Adapted From NIPP: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

**Risk Analysis**

DHS Risk Lexicon: The systematic examination of the components and characteristics of risk.

**Risk Assessment**

Adapted From DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 5: The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing, or comparing courses of action, and informing decision making. The appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes determining the extent to which adverse circumstances or events could result in harmful consequences.

**Risk Management**

From DHS Risk Lexicon and Adapted; CNSSI 4009, NIST SP 800-53 Rev 5: The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken. Includes: 1) conducting a risk assessment; 2) implementing strategies to mitigate risks; 3) continuous monitoring of risk over time; and 4) documenting the overall risk management program.

**Security Policy**

Adapted From CNSSI 4009, NIST SP 800-53 Rev 5, NIST SP 800-130, OASIS SAML Glossary 2.0: A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets. A rule or set of rules applied to an information system to provide security services.

**Security Program Management**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., the role of a Chief Information Security Officer).

**Strategic Planning and Policy Development**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Applies knowledge of priorities to define an entity.

**Supervisory Control and Data Acquisition**

Adapted From NCSD Glossary, CNSSI 4009: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

**Supply Chain**

Adapted From CNSSI 4009, NIST SP 800-53 Rev 5: A system of organizations, people, activities, information, and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

**Supply Chain Risk Management**

Adapted From DHS Risk Lexicon, CNSSD 505: The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

**System Administration**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability; also manages accounts, firewalls, and patches; responsible for access control, passwords, and account creation and administration.

**Systems Development**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Works on the development phases of the systems development lifecycle.

**Systems Requirements Planning**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions; provides guidance to customers about applicability of information systems to meet business needs.

**Tabletop Exercise**

Adapted From NCSD Glossary, DHS Homeland Security Exercise and Evaluation Program: A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements, or other information for managing an incident.

**Targets**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

**Test and Evaluation**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology.

**Threat**

Adapted From DHS Risk Lexicon, NIPP, CNSSI 4009, NIST SP 800-53 Rev 5: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

**Threat Agent**

Adapted From DHS Risk Lexicon: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

**Threat Analysis**

Adapted From DHS personnel; From NICE Framework: The detailed evaluation of the characteristics of individual threats. In the NICE Framework, cybersecurity work where a person: Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

**Threat Assessment**

From DHS Risk Lexicon and adapted From CNSSI 4009, NIST SP 800-53, Rev 5: The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

**Unauthorized Access**

From CNSSI 4009: Any access that violates the stated security policy.

**Virus**

Adapted from CNSSI 4009: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

**Vulnerability**

Adapted From DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 5: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. Characteristic of location or security posture or of design, security procedures, internal controls, or the implementation of any of these that permit a threat or hazard to occur. Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized.

**Vulnerability Assessment and Management**

From NICE Framework: In the NICE Framework, cybersecurity work where a person: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise, or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

**Worm**

From CNSSI 4009: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

### 1.2 Common Acronyms

|  |  |
| --- | --- |
| CDO | Chief Data Officer |
| CFAA | Computer Fraud and Abuse Act (1986) |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CJIS | Criminal Justice Information Services, a division of the FBI |
| CLIA | Clinical Laboratory Improvement Amendments |
| CPO | Chief Privacy Officer |
| CTO | Chief Technology Officer |
|  |  |
| FERPA | Family Educational Rights and Privacy Act (1974) |
| FISMA | Federal Information Security Management Act (2014) |
| FTI | Federal taxpayer information |
| HIPAA | Health Insurance Portability and Accountability Act (1996) |
| HITECH Act | Health Information Technology for Economic and Clinical Health Act (2009) |
| IRS | Internal Revenue Service |
| IRT | Incident Response Team |
| ISO | Information Security Office |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PHI | Personal Health Information |
| PIA | Public Information Act, Government Code Ch. 552 |
| PII | Personal Identifying Information |
| SPI | Sensitive Personal Information |
| SSA | Social Security Administration |

## SECTION 2 Incident Response Procedure

* 1. **Incident Response Procedure**

|  |
| --- |
| **Incident Response Procedure** |
|  |
| **1.0** **PURPOSE** |
|  |
| The purpose of this procedure is to define the requirements for an organization information security and privacy incident response capability.  A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in ***bold italics***. In addition, references to National Institute of Standards and Technology Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” family identifiers and control numbers are provided in parentheticals next to requirement headers, where applicable. |
| **2.0 SCOPE** |
|  |
| This procedure defines the requirements necessary to provide a coordinated information security incident response for all of [Name of Organization]. The requirements of this policy apply to all [Name of Organization] programs and include all [Name of Organization] ***-managed system assets***. |
| **3.0 BACKGROUND** |
|  |
| Information technology (IT) is an integral part of how [Name of Organization] conducts business and maintains information in support of its stated mission. Therefore, [Name of Organization] must be prepared to respond when information security and privacy incidents occur. Poorly handled incidents can result in compromised evidence, loss of time, conflicting information, negative publicity, and loss of data ***confidentiality***, ***integrity***, and ***availability***. Responses to an IT security incident can range from simply recovering compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning and ensuring that the right resources are available are critical to [Name of Organization]' ability to adequately detect, respond to and recover from an incident. |
| **4.0 REFERENCES** |
|  |
| **4.1 National Institute of Standards and Technology (NIST) Special Publication (SP)800-53, Security and Privacy Controls for Federal Information Systems and Organizations:**  NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal government information systems. |
|  |
| **4.2** **Ohio Administrative Policy IT-13, Data Classification**:  Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality. |
| **4.3 Ohio Administrative Policy IT-14, Data Encryption and Securing Sensitive Data**:  Ohio Administrative Policy IT-14 provides guidance to agencies as they take steps to protect sensitive data and information. |
| **4.4 Office of Information Technology (OIT) Enterprise IT Procedure OEP-SEC.4001, Statewide Incident Response Reporting**:  Defines the steps to be followed by State of Ohio agencies reporting information, computer system, privacy, or network security incidents. |
| **4.5 DAS Policy 200-14, Teleworking**:  DAS Policy 200-14 outlines the requirements for DAS teleworking. |
| **4.6 Ohio Revised Code 1347.15, Access rules for confidential personal information**: This section of Ohio Revised Code (ORC) outlines what needs to be included in the rules that each state agency adopts under Chapter 119 of the Revised Code, regulating access to the confidential personal information the agency keeps, whether electronically or on paper. |
| **4.7 State of Ohio IT Guideline, Information Technology Business Continuity Planning**: This IT guideline provides state agencies guidance in the development and implementation of a comprehensive IT business continuity plan that, in the event of a business disruption, will help enable the continuation of critical processes and the delivery of essential services at an acceptable level. |

|  |
| --- |
| **5.0 PROCEDURE** |
| All ***information security and privacy incidents*** shall be immediately reported to the [Name of Organization] [Insert how staff should report security or privacy incidents.] |
| The [Name of Organization] Technology Team will have an IRT and shall provide oversight for all information security and privacy incidents. The IRT shall define procedures for an information security and privacy incident response capability, which includes requirements for incident preparation, detection and analysis, containment, eradication and recovery, lessons learned analysis, records management, training, and testing. |
| 5.1 **Definition of Security and Privacy Incidents:** A security incident threatens the confidentiality, integrity, and / or availability of state information resources. Privacy incidents are a subset of security incidents for the purposes of this policy. Incidents may fall into one or more of following categories: |
| **5.1.1 Loss or Theft**: The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, storage device, or authentication ***token***. This may also include the loss/theft of hard copy documents containing ***sensitive data*** or ***personally identifiable information*** (***PII***). |
| ***5.1.2 Denial of Service* (DoS):** An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. Examples of these types of attacks include:   * Attacks, including physical attacks, which adversely affect or degrade access to critical services. * Persistent or significant DoS attacks (e.g., attempted attacks aimed specifically at DNS servers or routers). * Use of the organization’s devices to initiate or facilitate Distributed Denial of Service (DDoS) attacks. * Attempts, either failed or successful, to cause failures in critical infrastructure services or loss of critical ***supervisory control and data acquisition systems (SCADA)***. |
| **5.1.3 Improper Usage or Access**: Acceptable computing use or access laws, rules, or policies are violated. This includes suspected criminal use of systems or services, including, but not limited to identify theft and the disclosure, improper access, destruction, or alteration of any state managed systems or data. Improper usage or access includes potential violations of ORC Chapter 1347. |
| ***5.1.4 Information Spillage***: Information spillage refers to instances where sensitive information is inadvertently exposed to unauthorized disclosure. Information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. Examples include:   * Sensitive information placed on information systems that are not authorized to process such information; * Information thought to be public is posted on a state website, but is later determined to contain non-public data; * Non-public information added to a system, which is not accredited to host non-public information; and * Misdirected or improperly sent email or postal mail with sensitive information. |
| ***5.1.5 Malicious Code***: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.   * For the purposes of this policy, malicious logic that is successfully quarantined by antivirus software or that falls within normal or expected behaviors is not considered an incident. However, the organization needs to determine why the malicious code was there, and if a user was involved, the user needs to be educated. |
| **5.1.6 Phishing Messages**: Email containing malicious code designed to trick users into providing sensitive information (e.g. usernames, passwords, information that could be contained in a secret question like “What’s your pet’s name?”; or “What’s your mother’s maiden name?”, etc.).   * For the purposes of this policy, the organization needs to determine why the phishing email was opened, identify the user involved, and the user needs to be educated. |
| **5.1.7 Scans/Probes/Attempted Access**: Any activity that seeks to access or identify a state computer, open ports, protocols, service, or any combination for later exploitation. |
| **5.1.8 Social Engineering:** A bad actor working to trick a user into providing sensitive information (e.g., usernames, passwords, or any sensitive data, or physical access that the user can provide). |
| **5.1.9 Unauthorized Access:** To gain or attempt to gain logical or physical access, without permission, to a network, system, application, data, sensitive hard copy records, or other resource. This also includes changes to system, ***firmware***, hardware or software configuration characteristics without the state's knowledge, instruction, or consent. |
| **5.2 Incident Training Requirements (IR-2):** The IRT will provide basic incident response training and data privacy points of contact for incident response team members.    The IRT will provide training to security personnel at least annually, or when required by information system changes. Simulated events shall be incorporated into the training to facilitate effective response by personnel in crisis situations. Automated mechanisms shall be employed to provide a more thorough and realistic incident response training environment. |
| **5.3 Incident Testing Requirements (IR-3):** TheIRT shall conduct annual incident response testing exercises, which simulate incidents. These tests shall measure the effectiveness of the incident response capability and identify potential weaknesses. Tests shall be designed to stress the incident response capability and should leverage the use of automated tools as much as practical. |
| ***5.4 Incident Handling* (IR-4):** The IRT shall define procedures for an incident response capability, which includes security incident preparation, reporting, detection & analysis, containment, and eradication & recovery. These incident handling activities are combined with contingency planning activities, as needed. Lessons learned from ongoing incident handling activities are incorporated into incident response procedures, training, and testing. |
| **5.5 Incident Communication and Coordination Mechanisms**: The incident response capability established by the IRT shall include separate and different communication and coordination mechanisms in case of the failure of one mechanism. |
| * + 1. **Contact Information**: Contact information shall be captured for team members, law enforcement agencies, business partners and others within and outside of the organization (primary and backup contacts), including on call and escalation information. |
| * + 1. **Incident Reporting Mechanisms**: Incident reporting mechanisms shall be clearly defined (e.g., phone numbers, e-mail addresses, online forms, etc.). |
| * + 1. **Incident Tracking System**: An incident tracking system shall be utilized to record pertinent information about information security incidents. |
| * + 1. **Communication and Coordination Resource Needs**: The IRT shall determine the hardware, software and facilities needed to support the communication and coordination of incident response activities (e.g., smartphones, encryption software, war rooms, secure storage facilities, etc.). |
| **5.6 Incident Preparation:** Preparation is a key element of incident response. Refer to the State of Ohio IT Guideline, “Information Technology Business Continuity Planning,” for additional information. System owners shall maintain documentation, such as:   * Inventory of System Interconnections (Data Flows) * Data Sharing Agreement Inventory * Hardware Inventory, including asset specifics and owner (assigned to) information for mobile, endpoint, server, and virtual devices * Software Inventory * System Inventory, including system and business owner and contact information; operating, database, and application software; and physical and network location * Network Topology, including subnet information for endpoint, server, wireless and voice networks * Vendor Managed System Inventory, including system, vendor and business owner and contact information; operating, database, and application software; physical and network location; and contact information for the vendor security team * All enterprise assets should report to a common source for Network Time Protocol (NTP) * [Name of Organization] ***Insert BEFORE\_Incident Response Guide Planning Here- Incident Preparation Documentation Sheet*** |
| **5.7 Incident Response Risks**: The IRT shall evaluate what risks may be associated with a given IT security incident and develop procedures to ensure critical tools, data and equipment are available to facilitate containment and recovery. The procedures shall address: |
| * + 1. **Incident Response Contact List:** The IRT shall continue to maintain an incident response contact list, which contains names, desk phone numbers, mobile phone numbers, email addresses, organization names, titles, and incident response roles and responsibilities for all key incident response resources. These resources include, but are not limited to, key management personnel, public information officers, legal counsel, law enforcement officials, and organization incident response contacts. [Name of Organization] ***Insert BEFORE\_Incident Response Guide Planning Here- IRT Members by Roles and IRT Team***   **Incident Analysis Resources**: The IRT shall identify the resources that will be used as part of the incident response process. This includes the hardware and software that will be used for incident analysis (e.g., digital forensic workstations; laptops; spare workstations, servers and networking equipment or the virtualized equivalents; packet sniffers; removable media; etc.) as well as port lists; documentation for operating systems, applications, intrusion detection, and antivirus; network diagrams; lists of critical assets; current baselines; cryptographic hashes of critical files; etc. Automated mechanisms shall be used to support the incident handling process. [Name of Organization] ***Insert BEFORE\_Incident Response Guide Planning Here-Incident Analysis Resources Sheet*** |
| **5.8 Incident Reporting**: Incident reporting procedures are documented in Ohio Enterprise IT Procedure OEP-SEC.4001, “Statewide Incident Response Reporting.” |
| **5.9 Detection and Analysis:** The IRT shall provide guidance on how to detect and analyze incidents that use common attack vectors. |
| **5.10 Incident Containment**: The IRT shall quickly determine containment strategies in an effort to minimize damage. |
| **5.11 Evidence Preservation**: The IRT shall take appropriate steps to preserve sufficient evidence to ensure accurate incident records, facilitate the investigation and determine the extent of the damage. |
| **5.12 Eradication & Recovery**: The IRT procedures shall clearly convey when and how systems shall be restored to normal operation, confirm the systems are functioning normally, and, if applicable, remediate vulnerabilities to prevent similar incidents. All affected hosts shall be remediated. |
| **5.13 Lessons Learned**: After a major incident, the [Name of Organization] system or service owner shall hold a lessons learned meeting with all involved parties as soon as possible. A member of the IRT shall participate in these meetings as well as members of the impacted [Name of Organization] Community. |
| **5.14 Incident Response Team Responsibilities (IR-7):** IR Team responsibilities shall include, conducting training on incident response processes and procedures; leading incident response exercises; and engaging in proper incident handling, monitoring, and reporting as it pertains to incidents. The IRT shall ensure incidents are properly identified, contained, and remediated and to assist in recovery efforts. |
| **5.14.1** The IR team shall consist of the following core members or their designees:   * + Chief Technology Officer (CTO)   + Technology Department Admin Assistant   + System Administrator   + Network Administrator   + Building Technicians   + Teaching and Learning Coaches (Knowledge Managers)   + Data Coordinator |
| 5.15 **Information Security and Privacy Incident Response Team:** An information security and privacy incident response team shall include members from the Incident Response and the following representatives or their designees:   * + Chief Executive   + Chief Financial Officer/Treasure (CFO)   + Executive Director of Human and Material Resources   + Director of Communications   + Director of Facilities and Transportation   + Custodial Maintenance Supervisor   + Security Officer   + Legal Council |
| 5.16 **Incident Response Plan (IR-8):** The IRT shall develop, maintain, and distribute (as appropriate) an incident response plan. As a minimum, the plan shall contain the following elements:   * + Organization and structure of the enterprise information security and privacy incident response capability   + organization incident response roles & responsibilities   + Protocols for communication during incident response   + Guidance for incident evaluation (e.g., collection, analysis, classification, forensic/evidentiary considerations)   + Best practices for incident containment, eradication, recovery & reporting   + Lessons learned procedures   + Incident reporting metrics |
| **5.17 Incident Response Records Management**: The IRT shall monitor and maintain records of reported information security incidents. Guidance on maintaining incident response records is contained in section 6.0 Procedures. |
| **5.18 Personal Information Security Breach Notifications:** TheIRT shall work with organization information security and privacy incident response teams to ensure that incident notifications, including those under ORC 1347.12 and 1347.15 and any applicable federal regulations, are sent to the appropriate parties. |
| **5.18**.1 **Outside Entities**:If the incident resulted in a breach of a system containing data from an outside entity like the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Service (IRS), or the Social Security Administration (SSA), notifications must be made immediately, or within the timeframe of the applicable outside entity, but not more than 24-hours, to the external organization. Timely notification to affected individuals may also be required. |
| **6.0 PROCEDURES** |
| **6.1** **Maintaining Incident Response Security Records**: The IRT shall safeguard and restrict access to incident data because it often contains sensitive information. Incident response security records shall contain the following:    6.1.1 The current status of the incident, (e.g., new, in progress, forwarded for investigation, resolved, etc.)  6.1.2 A summary of the incident  6.1.3 Indicators related to the incident  6.1.4 Other incidents related to this incident  6.1.5 Actions taken by all incident handlers on this incident  6.1.6 Chain of custody, if applicable  6.1.7 Impact assessments related to the incident  6.1.8 Contact information for other involved parties (e.g., system owners, system administrators)  6.1.9 A list of evidence gathered during the incident investigation  6.1.10 Comments from incident handlers  6.1.11 Next steps (e.g., rebuild the host, upgrade an application) |
| **7.0 COMPLIANCE** |
|  |
| As of the effective date of this policy, IRT may not be completely aligned to the requirements outlined in the policy. A general implementation framework for the requirements of this policy includes: |
|  |

## SECTION 3 Privacy/Security Event Initial Triage Checklist

1. **Incident Response Team:** Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident. Meet daily, if necessary, with priority over other work, possibly requiring after-hours activities.
2. **Secure data:** Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate, e.g. harden or disable system or contact internet search engines if appropriate to clear internet cache.
3. **Data elements:** Determine the types, owners, and amounts of confidential information that were possibly compromised.
4. **Data source:** Identify each location where confidential information may have been compromised and the business owner of the confidential information.
5. **Scope and escalation:** Confirm the level and degree of unauthorized use or disclosure (includes access) by the named or unidentified individuals or threats.
6. **Number of individuals impacted:** Determine the number of individuals impacted. The number may implicate breach notification requirements, e.g. individual or media notice.
7. **Discovery date:** Determine the date the organization or contractor knew or should have known about the event/incident.
8. **Management alert:** Advise appropriate internal management.
9. **External communications, as required:** Advise external contacts, such as DIR, legislative leadership, the Office of the Inspector General, the Office of the Attorney General, Secretary of State (SOS) (if election data involved), law enforcement, outside counsel, and applicable regulatory authorities.
10. **Investigate:**
    1. Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.
    2. Documents: Gather and review contracts and provisioning documents (documents authorizing access or restricting use or disclosure).
    3. Root Cause Analysis: Prepare RCA which describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence.
    4. Event and Threat Impact Analysis (see section on Event Threat and Impact Analysis below).
11. **Mitigation:** Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence. Set a timeline and assign responsibility to ensure accountability. Follow-up to ensure corrective action initiated and completed on time or decision to accept the risk of recurrence, and report appropriately.

## SECTION 4 Event Threat, Impact Analysis, and Escalation Criteria

The investigation of the incident/event should include an Event Threat and Impact Analysis to accurately categorize the impact of the event on the organization. Once the event’s impact level is understood it may be appropriate to escalate the incident response and contact other entities.

### 4.1 Event Threat and Impact Analysis

The National Institute of Standards and Technology (NIST) Special Publication [NIST 800-61,](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf) Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include:

* **Functional Impact.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.
* **Information Impact.** Incidents may affect the confidentiality, integrity, and availability of the organization’s information.
* **Recoverability.** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

While there is no single model for determining event impact, the below tables provide guidance on defining impact to organization systems, organization information (business impact), and organization ability to recover from an event (possible responses). Organizations should consider each category to assure proper response and recovery from these events.

**Table 4.1: Examples of functional impact categories**

|  |  |
| --- | --- |
| **Category** | **Definition** |
| **None** | No effect to the organization’s ability to provide all services to all users. |
| **Low** | Minimal effect: the organization can still provide all critical services to all users but has lost efficiency. |
| **Medium** | Organization has lost the ability to provide a critical service to a subset of system users. |
| **High** | Organization is no longer able to provide some critical services to any users. |

**Table 4.2: Examples of possible information impact categories**

|  |  |
| --- | --- |
| **Category** | **Definition** |
| **None** | No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| **Privacy Breach** | Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| **Proprietary Breach** | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes. |
| **Integrity Loss** | Sensitive or proprietary information was changed or deleted accidentally or intentionally. |

**Table 4.3: Examples of recoverability effort categories**

|  |  |
| --- | --- |
| **Category** | **Definition** |
| **Regular** | Time to recovery is predictable with existing resources |
| **Supplemented** | Time to recovery is predictable with additional resources |
| **Extended** | Time to recovery is unpredictable; additional resources and outside help are needed |
| **Not recoverable** | Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly), launch investigation. |

### 4.2 Event Escalation: Communication

[NIST 800-61 C](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf)omputer Security Incident Handling Guide provides advisement on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications.

**Key Contacts.** Organizations should establish an escalation process for instances when key individuals outside of normal technical response processes must be notified. Among those to be considered are:

* Other incident response teams within the organization
* External (contractor) incident response teams, if appropriate
* Board
* Human resources
* Public affairs
* Legal Counsel
* US-CERT (required for systems operated on behalf of the federal government)
* Law enforcement, if appropriate
* Federal government agencies, if appropriate
* Department of Information Resources Office of the CISO (Mandated for Ohio Agencies)

***Insert BEFORE\_Incident Response Guide Planning Here-Key Contacts Sheet***

**Contact Methods.** Organizations may need to provide status updates to certain external and internal parties. Among communication methods to be considered are:

* Email (only if integrity of the email is verified as good)
* Website (internal, external, or portal)
* Telephone calls
* In person (e.g., daily briefings)
* Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk’s voicemail greeting)
* Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

## SECTION 5 Breach Notice Criteria

Certain types of breaches carry legal notification responsibilities. This section includes information about breach notification statutes and rules according to Ohio law, federal laws and regulations, and other states’ laws.

* Enacted in 2005, Ohio’s data breach notification law requires entities that conduct business in Ohio and that own or license computerized personal information, to notify Ohio residents of any data breach that does result or could result in the unauthorized access and acquisition of their unencrypted or unredacted personal information that is likely to cause a risk of identity theft or fraud.
* Notice must be made in the most expedient time possible, no later than 45 days after discovery or notification of the breach. Breached third parties must notify the relevant data owners or licensees as well.
* If more than 1,000 individuals have to be notified of a breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, unless they are covered by [HIPAA](https://www.itgovernanceusa.com/hipaa).
* Substitute notice is permitted in specific circumstances and notification may be delayed for law enforcement purposes.
* Financial institutions compliant with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice are deemed to comply with this law.
* Organizations can use Table 5.3 to report data breaches to other states.

**Table 5.1: Ohio legal requirements for breach notices**

|  |  |  |
| --- | --- | --- |
| **Breach Notice** | **Citation** | **Requirement** |
| [Ohio Revised Code](https://codes.ohio.gov/ohio-revised-code) / [Title 13 Commercial Transactions](https://codes.ohio.gov/ohio-revised-code/title-13) / [Chapter 1347 Personal Information Systems](https://codes.ohio.gov/ohio-revised-code/chapter-1347) | Section 1347.12 | Agency disclosure of security breach of computerized personal information data. | (B)(1) Any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the state agency or agency of a political subdivision with any person or another state agency or agency of a political subdivision prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the state agency or agency of a political subdivision is in this state.  (2) The state agency or agency of a political subdivision shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.  (C) Any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information shall notify that other state agency or agency of a political subdivision of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.  (D) The state agency or agency of a political subdivision may delay the disclosure or notification required by division (B), (C), or (F) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the state agency or agency of a political subdivision shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.  (E) For purposes of this section, a state agency or agency of a political subdivision may disclose or make a notification by any of the following methods:  (1) Written notice;  (2) Electronic notice, if the state agency's or agency of a political subdivision's primary method of communication with the resident to whom the disclosure must be made is by electronic means;  (3) Telephone notice;  (4) Substitute notice in accordance with this division, if the state agency or agency of a political subdivision required to disclose demonstrates that the agency does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following:  (a) Electronic mail notice if the state agency or agency of a political subdivision has an electronic mail address for the resident to whom the disclosure must be made;  (b) Conspicuous posting of the disclosure or notice on the state agency's or agency of a political subdivision's website, if the agency maintains one;  (c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state.  (5) Substitute notice in accordance with this division, if the state agency or agency of a political subdivision required to disclose demonstrates that the agency has ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following:  (a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the state agency or agency of a political subdivision is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;  (b) Conspicuous posting of the disclosure or notice on the state agency's or agency of a political subdivision's website, if the agency maintains one;  (c) Notification to major media outlets in the geographic area in which the state agency or agency of a political subdivision is located.  (F) If a state agency or agency of a political subdivision discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the state agency or agency of a political subdivision shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the state agency or agency of a political subdivision to the residents of this state. In no case shall a state agency or agency of a political subdivision that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.  (G) The attorney general, pursuant to sections [1349.191](https://codes.ohio.gov/ohio-revised-code/section-1349.191) and [1349.192](https://codes.ohio.gov/ohio-revised-code/section-1349.192) of the Revised Code, may conduct an investigation and bring a civil action upon an alleged failure by a state agency or agency of a political subdivision to comply with the requirements of this section. |
| [Ohio Revised Code](https://codes.ohio.gov/ohio-revised-code) / [Title 13 Commercial Transactions](https://codes.ohio.gov/ohio-revised-code/title-13) / [Chapter 1349 Consumer Protection](https://codes.ohio.gov/ohio-revised-code/chapter-1349) | Section 1349.19 | Private disclosure of security breach of computerized personal information data. | (B)(1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.  (2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.  (C) Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of this state.  (D) The person may delay the disclosure or notification required by division (B), (C), or (G) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.  (E) For purposes of this section, a person may disclose or make a notification by any of the following methods:  (1) Written notice;  (2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means;  (3) Telephone notice;  (4) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall consist of all of the following:  (a) Electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made;  (b) Conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one;  (c) Notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds seventy-five per cent of the population of this state.  (5) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall consist of all of the following:  (a) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;  (b) Conspicuous posting of the disclosure or notice on the business entity's web site, if the entity maintains one;  (c) Notification to major media outlets in the geographic area in which the business entity is located.  (F)(1) A financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the requirements of this section.  (2) This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103, as amended.  (G) If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.  (H) Any waiver of this section is contrary to public policy and is void and unenforceable.  (I) The attorney general may conduct pursuant to sections [1349.191](https://codes.ohio.gov/ohio-revised-code/section-1349.191) and [1349.192](https://codes.ohio.gov/ohio-revised-code/section-1349.192) of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section. |
| [Ohio Revised Code](https://codes.ohio.gov/ohio-revised-code) / [Title 13 Commercial Transactions](https://codes.ohio.gov/ohio-revised-code/title-13) / [Chapter 1349 Consumer Protection](https://codes.ohio.gov/ohio-revised-code/chapter-1349) | Section 1349.191 | Investigation of noncompliance with disclosure laws | (B) The attorney general may conduct an investigation if the attorney general, based on complaints or the attorney general's own inquiries, has reason to believe that a state agency or an agency of a political subdivision has failed or is failing to comply with section [1347.12](https://codes.ohio.gov/ohio-revised-code/section-1347.12) of the Revised Code or that a person has failed or is failing to comply with section [1349.19](https://codes.ohio.gov/ohio-revised-code/section-1349.19) of the Revised Code. |
| [Ohio Revised Code](https://codes.ohio.gov/ohio-revised-code) / [Title 13 Commercial Transactions](https://codes.ohio.gov/ohio-revised-code/title-13) / [Chapter 1349 Consumer Protection](https://codes.ohio.gov/ohio-revised-code/chapter-1349) | Section 1349.192 | Civil action by attorney general for violation of disclosure laws | (A)(1) The attorney general shall have the exclusive authority to bring a civil action in a court of common pleas for appropriate relief under this section, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a state agency or an agency of a political subdivision has failed or is failing to comply with section [1347.12](https://codes.ohio.gov/ohio-revised-code/section-1347.12) of the Revised Code or that a person has failed or is failing to comply with section [1349.19](https://codes.ohio.gov/ohio-revised-code/section-1349.19) of the Revised Code. Upon its finding that a state agency or an agency of a political subdivision has failed to comply with section [1347.12](https://codes.ohio.gov/ohio-revised-code/section-1347.12) of the Revised Code or that a person has failed to comply with section [1349.19](https://codes.ohio.gov/ohio-revised-code/section-1349.19) of the Revised Code, the court shall impose a civil penalty upon the state agency, agency of a political subdivision, or person as follows:  (a) For each day that the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section, subject to divisions (A)(1)(b) and (c) of this section, a civil penalty of up to one thousand dollars for each day the agency or person fails to comply with the section;  (b) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than sixty days, subject to division (A)(1)(c) of this section, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency or person fails to comply with the section and, for each day commencing with the sixty-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to five thousand dollars for each such day the agency or person fails to comply with the section;  (c) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than ninety days, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency or person fails to comply with the section, a civil penalty of up to five thousand dollars for each day commencing with the sixty-first day and continuing through the ninetieth day that the agency or person fails to comply with the section, and, for each day commencing with the ninety-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to ten thousand dollars for each such day the agency or person fails to comply with the section. |

**Table 5.2: Federal legal requirements for breach notices**

|  |  |  |  |
| --- | --- | --- | --- |
| **Breach Notice** | **Citation** | **Requirement** | **Notes** |
| **HIPAA** | 45 CFR §164.404 | Notify individual or Covered Entity of a breach of unsecured protected health information which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach. | Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice. |
| **Federal Financial Participation** | CMS SMELL #06- 022 | CMS-regulated entities must notify CMS within one clock hour according to Sep. 2006 CMS letter to State Medicaid Directors | Unclear if HIPAA HITECH eliminated the CMS requirement. SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or recipient is limited to use or disclosure “directly in connection with program administration,” but have no breach notice requirement. |
| **Internal**  **Revenue**  **Service** | By data sharing agreement with the IRS, pursuant to [IRS Publication 1075 §10](http://www.irs.gov/pub/irs-pdf/p1075.pdf) | Notify TIGTA and IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals. | The IRS Office of Safeguards may require individual notification. |
| **Social Security**  **Administration**  **(SSA)** | By contract between SSA and Agency which defers to [IRS Publication 1075](http://www.irs.gov/pub/irs-pdf/p1075.pdf) | Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any. | SSA may require individual notification. |
| **Federal Trade Commission (FTC)** | Health Breach Notification (PHR, EHR Vendors) [16 CFR Part 318](http://www.gpo.gov/fdsys/pkg/CFR-2012-title16-vol1/pdf/CFR-2012-title16-vol1-part318.pdf) | Requires a vendor of personal health records to notify the individual US Citizen and the FTC following the discovery of a breach of security of unsecured PHR- identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR- related entity. | Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. “Breach” is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60 calendar days after the breach discovery. |
| **Family**  **Educational**  **Rights and**  **Privacy Act**  **(1974)** | [20 USC §1232g,](http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf)  [34 CFR Part 99](https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl) | None. FERPA guidance recommends having breach response plans. | Applies to educational institutions regarding the privacy of personally identifiable information contained in education records of students. Consent is generally required to disclose education records. |

**State Data Breach Notification Laws:** The National Conference of State Legislatures maintains a [matrix of state data breach laws. A](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)s of April 2019, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

**Table 5.3: Security breach notification statute in Ohio.**

|  |  |
| --- | --- |
| **State** | **Citation** |
| **Ohio** | Ohio Rev. Code §§ [1347.12,](http://codes.ohio.gov/orc/1347.12) [1349.19,](http://codes.ohio.gov/orc/1349.19) [1349.191,](http://codes.ohio.gov/orc/1349.191) [1349.192](http://codes.ohio.gov/orc/1349.192) |

## SECTION 6 Post-Incident Checklist

The Computer Security Incident Handling Guide ([NIST 800-61)](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf) provides advisement on event analysis activities. Per section 3.4.1 (Lessons Learned) and section 3.4.2 (Using Collected Incident Data) relevant factors for post-incident and root cause analysis include:

1. **Learning and improving.** Incident Response Teams should hold “lessons learned” meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
   1. Exactly what happened, and at what times?
   2. How well did staff and management perform? Were documented procedures followed?
      1. Were procedures adequate?
   3. What information was needed sooner?
   4. Were any steps or actions taken that might have inhibited the recovery?
   5. What would/should staff, and management do differently the next time a similar incident occurs?
   6. How could information sharing with other organizations have been improved?
   7. What corrective actions can prevent similar incidents in the future?
   8. What precursors or indicators should be watched for in the future to detect similar incidents?
   9. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
2. **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
   1. Creating a formal event chronology (including time-stamped information from systems);
   2. Compiling a monetary estimate of the amount of damage the incident caused;
   3. Retaining follow-up reports as specified in retention policies.
3. **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.
4. **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
   1. Reviewing of logs, forms, reports, and other incident documentation;
   2. Identifying recorded precursors and indicators;
   3. Determining if the incident caused damage before it was detected;
   4. Determining if the actual cause of the incident was identified;
   5. Determining if the incident is a recurrence of a previous incident;
   6. Calculating the estimated monetary damage from the incident;
   7. Measuring the difference between initial impact assessment and the final impact assessment; and
   8. Identifying measures, if any, that could have prevented the incident.

## SECTION 7 Incident Response Team Templates

### 7.1 Title and Contact Information for Plan Sponsor/Owner

For questions or further information, please contact:

### 7.2 IRT Charter

**Information Privacy or Security Incident Response Team Charter**

**Charter Purpose:**

This Incident Response Team (the “IRT”) Charter establishes membership, subject matter experts, roles, responsibilities, and activities of the IRT to respond to an actual or suspected information privacy or security event/incident.

**IRT Mission:**

The IRT mission is, first, to prevent incidents by reasonably anticipating, detecting, and planning for actual and suspected privacy or security events; and second, to respond to and mitigate privacy or security events.

**Overview:**

The Incident Response Team (the “IRT”) is a standing team of internal personnel established by Leadership Team in this [Charter] with expertise in responding to a significant actual or suspected privacy or security event or incident. The IRT operates on behalf of Leadership Team and engages, informs, and receives support from Leadership Team. There [is/is not] a set protocol to initiate the IRT activities in response to an actual or suspected event/incident. Once activated, the IRT has authority to [request cooperation/establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours].

**Responsibilities and Roles:**

Responsibilities:

1. **Anticipate and prepare** the organization for privacy or security events/incidents which can be reasonably anticipated;
2. **Respond** to actual or suspected events/incidents on behalf of the organization as needed, with activities such as:
   1. Triage (see section 2);
   2. Communication, internal and external, as needed according to the organization's’s] communications protocol (e.g. funneled to the top from a deputy, for example)

(see communications templates)

* 1. Track and document IRT activities and discoveries; and
  2. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

* Uncontained or escalating malware attack on system (computer virus, worm, bot, or Trojan);
* Abuse, theft, misuse, or loss of data or hardware (including unauthorized use, disclosure, or access to computer accounts, systems, or data; hacking; human error);
* Improper use or disclosure of information or information resources as outlined in the organization's standards or contracts including e-mail, equipment, Internet, and acceptable data use
  + (includes human resources or contractor misuse or error);
* Many individuals or a large amount of sensitive data impacted; or
* Events likely to be high-profile or create a significant risk of individual harm (e.g., risk of financial harm, reputational harm, or medical identity theft).

Roles:

1. **The IRT Lead.** The Lead of the IRT may:
2. Be designated by and reporting to the Leadership Team. The IRT is led by Chief Technology Officer or his or her designee.
3. Declare an incident
4. Establish, maintain, and update written IRT protocols or incident response plans
5. Identify roles and responsibilities for IRT standing members
6. Request or designate ad hoc members for particular events as needed
7. [request cooperation / establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours]
8. **IRT Standing Members.** The standing members include named individuals or representatives.
9. **Ad hoc Members or Subject Matter Experts.** Ad hoc members or Subject Matter Experts may be designated as ad hoc resources by the IRT Lead.

### 7.3 IRT Membership by Roles

The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

**Standing IRT Membership Contact Information**

***Insert BEFORE\_Incident Response Guide Planning Here- IRT Members by Roles Sheet***

***OR complete table***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standing Members** | **Name** | **Phone** | **Email** | **After-hours contact** |
| IRT Lead |  |  |  |  |
| [Chief Technology Officer/Technology Director or designee] |  |  |  |  |
| [Network Administrator] |  |  |  |  |
| [Systems Administrator] |  |  |  |  |
| [Technology Administrative Assistant] |  |  |  |  |
| [Building Technicians] |  |  |  |  |
| [Teaching and Learning Coaches] |  |  |  |  |
| [Data Coordinator] |  |  |  |  |
| [Other] |  |  |  |  |
| Legal Counsel to the IRT – to avoid losing attorney-client  privilege, *do not list legal as a*  *member* |  |  |  |  |

**7.4 Supply Chain Membership by Roles**

The following table contains contact information for current Supply Chain members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her.

**Standing Supply Chain Membership Contact Information -**

***Insert BEFORE\_Incident Response Guide Planning Here- Supply Chain (Vendor List) Sheet***

***OR complete table***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standing Members** | **Name** | **Phone** | **Email** | **After-hours contact** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 7.5 IRT Meeting Minutes

***CONFIDENTIAL***  **Meeting Minutes for the organization's IRT Meeting , 20**

***Purpose:*** The purpose of this message is to provide updates regarding the IRT activities in response to confirmed privacy and/or security incidents involving personal or confidential information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action. This Alert will be regularly updated as more information becomes available.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Summary*** | | | |
| **Brief Incident Summary** | | | |
|  | | | |
| **Participants** | | | |
| **IRT Members Present:** | | |  |
| **IRT Members Not in Attendance:** | | |  |
| **Guests:** | | |  |
| **Current Updates** | | | |
| 1. |  | | |
| 2. |  | | |
| 3. |  | | |
| **Prior Updates** | | | |
| 1. |  | | |
| 2. |  | | |
| 3. |  | | |
| **Next Steps** | | | |
| 1. |  | | |
| 2. |  | | |
| 3. |  | | |
| **Next Scheduled Meeting** | |  | |
| **Location** | |  | |
| **Conference #** | |  | |
| **Access Code** | |  | |
|  | | | |

### 7.6 IRT Action List

**IRT: Identification Name or Number**

**Action Items Status**

**Current Updates as of . , 20**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Item** | **Date** | **Action** | **Assigned To** | **Assigned By** | **Status** |
| 1. |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |
| 6. |  |  |  |  |  |  |

### 

### 7.7 IRT State Government Contact Information

**IRT State Government Contact Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity** | **Contact** | **Division/Location** | **Email/Office Telephone** |
| **Office of the Governor** | Governor Mike DeWine | Riffe Center, 30th Floor,  77 South High Street,  Columbus, OH 43215-6117 | (614) 466-3555 |
| **Lieutenant Governor** | Lt. Governor Jon Husted | Riffe Center, 30th Floor,  77 South High Street,  Columbus, OH 43215-6117 | (614) 466-3555 |
| **Speaker of the House** | Robert R. Cupp | 77 South High Street, 13th Floor, Columbus, OH 43215 | (614) 466-9624 |
| **State of Ohio Office of the Chief Information Officer** | Ervan Rodgers II | 30 E. Broad St., 39th Floor Columbus, Ohio 43215 | (614) 466-6930 [state.cio@das.ohio.gov](mailto:state.cio@das.ohio.gov) |
| **State of Ohio Office of the Chief Information Officer, State CIO/Assistant Director** | Katrina Flory | 30 E. Broad St., 39th Floor Columbus, Ohio 43215 | (614) 644-6446 [Katrina.Flory@das.ohio.gov](mailto:Katrina.Flory@das.ohio.gov) |
| **State of Ohio Office of the State CIO, Deputy State CIO** | Kristina Hagberg | 30 E. Broad St., 39th Floor Columbus, Ohio 43215 | (614) 644-9245 [Kristina.Hagberg@das.ohio.gov](mailto:Kristina.Hagberg@das.ohio.gov) |
| **State of Ohio Office of Information Security and Privacy, Chief Information Security Officer** | Anupam Srivastava | 30 E. Broad St., 39th Floor Columbus, Ohio 43215 | 614-728-4504 [state.isp@das.ohio.gov](mailto:state.isp@das.ohio.gov) |

## SECTION 8 Additional Templates

### 8.1 Identity Theft Protection Criteria

Although it is optional for a state agency to provide identity theft protection, each agency should evaluate the risk of financial or medical identity theft occurring. If the risk is deemed significant, the agency may consider this type of protection. In addition to deciding whether to provide the protection, an agency should consider an appropriate length of time to provide the protection. Ultimately the decision to provide protection should be made at an Executive-level position. Should an agency determine identity theft protection is appropriate, there are various types and level of protection to choose from on the market, including:

* Identity theft insurance with various coverages or guarantees
* Credit report monitoring
* Claims monitoring
* Monitoring of websites used to trade stolen information
* Theft assistance resolution

As noted, commercial identity theft protection varies in the means and extent of coverage. While some carriers offer compensation for expenses incurred as a result of theft, others simply provide credit monitoring and alerts to an individual in the event of credit activity. In addition to assistance for affected individuals, breach management services can be procured to assist an entity responsible for a breach, as well as provide risk assessment, mitigation, or remediation services. As circumstances warrant, the organization may elect to procure commercially available identity theft protection or breach management services, especially for high-profile events likely to lead to significant harm to impacted individuals or reputational harm or cost to the organization.

The organization will consider the following criteria to determine whether to procure identity theft protection or breach management services:

1. Contract opportunities made available to state agencies by the Department of Information Resources for identity theft or breach management services [see resources page].
2. Contractual requirements imposed upon the organization's vendor or contractor, or other third party responsible for the breach, to provide identity theft protection, breach management services to the agency, or any other indemnification or hold harmless contract provisions.
3. Degree and scope of the breach and the degree or type of risks to individuals, such as financial, reputational, or other harm (such as medical identity theft or criminal identity theft), dependent upon the various forms of identity theft.
4. The extent to which commercial services will be unable to detect or deter harm such as medical or criminal identity theft for the breach at issue.
5. No or low-cost measures available to impacted individuals to protect themselves, such as a self-imposed credit fraud alert, a credit freeze request to one of the credit bureaus [see breach notice template for more information] or filing a police report. Some options for impacted individuals include:
   1. A fraud alert which can help prevent an identity thief from opening additional accounts in a consumer’s name in 90 days.
   2. A security freeze, also known as a credit freeze, which is a warning sign to businesses or others who may use an individual’s credit file and requires a police report.
   3. Contacting the Consumer Protection Division of the Ohio Office of the Attorney General.
   4. The ability to link the breach event to an identity theft event or other harm.
   5. The cost to the agency or agency contractor for the provision of identity theft or breach management services.

**8.2 Internal Management Alert Template**

**Warning: Email communication may be compromised and should not be used until verified that email is safe.**

***NOTICE: The information contained in this message and any attachment to this message are confidential under state or federal law and may be protected by attorney-client privilege. If you have received this message in error, please immediately notify the sender of this e-mail, then delete or destroy it and any attachment(s). Thank you.***

**Agency Data Security Incident Alert**

***Purpose:*** The purpose of this message is to inform you of a suspected or confirmed privacy and/or security incident involving personal information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action and will be regularly updated as more information becomes available.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Summary*** | | | |
| **Brief Incident Summary** | | | |
|  | | | |
| **Participants** | | | |
| **IRT Members Present:** | | |  |
| **IRT Members Not in Attendance:** | | |  |
| **Guests:** | | |  |
| **Immediate Recommendations** | | | |
| 1. |  | | |
| 2. |  | | |
| 3. |  | | |
| **Next Steps** | | | |
| 1. |  | | |
| 2. |  | | |
| 3. |  | | |
| **Next Scheduled Meeting** | |  | |
| **Location** | |  | |
| **Conference #** | |  | |
| **Access Code** | |  | |
|  | | | |

### 8.3 Notice to Individuals Affected by Incident

Warning: Your legal council should review communication to affected individuals.

<Date>

<<Title>> <<First Name>> <<Last Name>>

<<Address>>

<<City>>, OH. <<Zip>>

Dear <<Title>> <<Last Name>>:

Your name and certain personal information was [exposure type/description]. This means that information may have been exposed without your authorization or the authorization of the organization. We apologize for any inconvenience this offers you. [Although there is no evidence that any information has been misused, the state is providing you with free credit monitoring coverage.]

[Describe the incident and what the agency is doing to mitigate the incident.]

We are committed to helping you safeguard your information. [The organization is providing you with free credit monitoring and identity theft services for one year. This service includes an insurance policy of up to $[ ] in identity theft coverage, a year of [name of Agency’s contracted Breach Management Vendor product] coverage, and a full-service identity restoration team to guide you through the recovery process if anyone tries to misuse your information. You must enroll to take advantage of this free service.]

We have set up a website that will help you protect your information and will provide you with updates on this matter. You may also call [name of Agency’s contracted Breach Management Vendor] to ask for help in keeping your data safe. **If you are enrolling a minor child, you will need to call [Breach Management Vendor] to process their enrollment manually. Child enrollment cannot be conducted online.**

We recommend that you also take the following steps to protect your identity:

* Contact one of the national credit reporting agencies below and ask for a fraud alert on your credit report. The agency will alert all other agencies. Remember to renew these fraud alerts every 90 days. The state does not have authority to do this for you, as the credit bureaus must have your permission to set up the alerts.
* The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You may contact each agency to determine if a child has a file or if the child’s information has been misused:

|  |  |
| --- | --- |
| **Equifax**  1550 Peachtree St NW  Atlanta, GA, 30309-2468 | [www.equifax.com](http://www.equifax.com)  800-525-6285 |
| **Experian**  P.O. Box 2002  Allen, TX 75013 | [www.experian.com](http://www.experian.com)  Fraud Hotline (toll-free): 1-888-397-3742 |
| **TransUnion**  P.O. Box 6790  Fullerton, CA 92834 | [www.transunion.com](http://www.transunion.com)  Fraud Hotline (toll-free): 1-800-680-7289  Report fraud: fvad@transunion.com |

You are entitled to receive one free credit report from each of the three national credit reporting agencies once per year. To request a copy of your free credit report, visit

[www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877-322-8228.

* Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.
* Monitor your [bank account activity / health care records / medical insurance company explanation of benefits] to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to your [bank / health care provider / health insurance company’s privacy officer].
* Report any suspicious activities on your [credit reports or bank account / health care or health insurance records] to your local police or sheriff’s office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.
* Learn about the Federal Trade Commission’s identity theft programs by visiting [www.ftc.gov/bcp/edu/microsites/idtheft o](http://www.ftc.gov/bcp/edu/microsites/idtheft)r by contacting the Federal Trade Commission’s toll-free Identity Theft helpline at 1-877-ID-THEFT (1-877-438-4339); TTY: 1-866-653-4261.
* [Enroll in free credit monitoring and identity theft services provided by the state. There is no cost to you for the service, but **you must enroll**. You can enroll online at or by contacting [Agencies contracted Breach Management Vendor’s] Customer Care Center toll- free at .]
* **[To enroll your minor child, please call [Agencies contracted Breach Management Vendor’s] Customer Care Center at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to manually enroll them. Child enrollments cannot be conducted online.]**
* Monitor the website at [organization’s contracted Breach Management Vendor’s agency / Agency’s own site] for periodic updates.

The organization regrets that this action is necessary. Please be assured that we are committed to helping you protect your credit and identity and in ensuring that your information is safe and secure.

If you have any questions, please call [Agency contact] at or contact by email at .

Sincerely,

[Authorized signatory]

### 8.4 Public (Media) Notice

Public notification should be made through normal PR channels.

[Name of Organization] Communications Steps

In the event that you choose to notify the public at large, the information in your notice should mirror the information contained in the breach notice to individuals affected (section 7.3). Media notice may be legally required; please see Breach Notice Criteria. A media notice should be developed through your usual public communication processes and contain the following information:

* Brief description of the details of the event
* Description of the individuals affected in the aggregate
* Description of actions taken by the organization
* Statement as to whether evidence indicates the data may have been misused
* Contact information for questions

**8.5 Post-Mortem and Improvement Plan**

INCIDENT POST-MORTEM

|  |  |
| --- | --- |
| **Cyber Incident** | [Use your organization’s naming convention of the incident] |
| **Start Date and Time** | [Indicate at a minimum the start date and time of the incident. Include a full incident chronology if available |
| **Detection Date and Time** | [Indicate at a minimum the detection date and time of the incident. Include a full incident chronology if available |
| **End Date and Time** | [Indicate at a minimum the end date and time of the incident. Include a full incident chronology if available |
| **Description** | [Give a brief description of the incident.] |
| **Impact** | [What was the impact to the organization?] |
| **Detection** | [How was the incident detected?] |
| **Learning and Improving** | |  |  |  | | --- | --- | --- | | **Question** | **Response** | **Comment** | | **How well did the staff and management perform?** |  |  | | **Were documented policy and procedures followed?** |  |  | | **Were the procedures adequate?** |  |  | | **Was the actual cause identified?** |  |  | | **What information was needed sooner?** |  |  | | **Were any steps taken that might have inhibited recovery?** |  |  | | **What should/would staff/management do differently the next time a similar incident happens?** |  |  | | **How could information sharing (in/out) with other organizations have been improved?** |  |  | | **What corrective actions can prevent or lower the likelihood of similar incidents in the future?** |  |  | | **What precursors or indicators of compromise should be watched in the future to speed up detection?** |  |  | | **What additional tools and/or resources are needed to address future incidents?** |  |  | | **What tools, processes, metrics, or resources could be in place and/or monitored to detect a similar incident sooner?** |  |  | |
| **Root Cause Analysis** | |  |  |  | | --- | --- | --- | | **Question** | **Response** | **Comment** | | **What could have prevented the incident?** |  |  | | **Was there damage caused prior to detection?** |  |  | | **Is the incident a recurrence of a previous incident?** |  |  | | **Was the actual cause identified?** |  |  | | **Was the actual cause identified?** |  |  | | **Were there any leading edge indicators of detection that were missed?** |  |  | |
| **Metrics** | [Enter any related metrics e.g. mean-time-to-incident-discovery, cost of recovery, time from detection to containment,…] |
| **Approximate cost of the incident** | [What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, organization downtime, idle employee time, backlog catchup overtime, etc.] |

**IMPROVEMENT PLAN**

This improvement plan has been developed specifically for [Organization] as a result of the Cyber Incident that occurred on [date].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Issue/Area for Improvement** | **Corrective Action** | **Primary Responsible** | **Start**  **Date** | **Completion Date** |
| 1. [Area for Improvement] | [Corrective Action 1] |  |  |  |
| [Corrective Action 2] |  |  |  |
| [Corrective Action 3] |  |  |  |
| 1. [Area for Improvement] | [Corrective Action 1] |  |  |  |
| [Corrective Action 2] |  |  |  |

### SECTION 9 External Contacts

**External Partners.** Collaboration with external entities may be necessary to assist with incident response or for auxiliary support. The IRT shall ensure that all those participating in the incident response work together efficiently and effectively.

The tables below identify contact information of external partners with whom the organization may need to collaborate in the event of an Incident as well as resource pages and other useful information.

#### Table 9.1: State of Ohio Contacts

|  |  |  |
| --- | --- | --- |
| **Resource** | **Services** | **Contact Information** |
| **Ohio Bureau of Criminal Investigation**  **Cyber Crimes Unit** | The unit helps local officials deal with the increasingly complex technical and legal issues involved in computer crime investigations and prosecutions. Its investigations encompass murder, sexual assault, fraud, theft, child pornography and other crimes committed with the aid of computers, external drives, memory cards, cellphones, digital cameras, gaming stations, global positioning systems and more. Most of the crimes investigated by the unit involve violent criminal activity, and more than half involve children. | Headquarters Bureau of Criminal Investigation  P.O. Box 365  London, OH 43140  740-845-2000  Athens Office  86 Columbus Circle, Suite 202  Athens, OH 45701  740-249-4378  Bowling Green Office  750 N. College Drive  Bowling Green, OH 43402  419-353-5603  Cambridge Office  1225 Woodlawn Avenue  Cambridge, OH 43275  740-845-2000  Richfield Office  4055 Highlander Parkway  Richfield, OH 44286  330-659-4600  Youngstown Office  20 W. Federal Street  Youngstown, OH 44503  330-884-7555 |
| **Ohio Office of the**  **Attorney General** | The agency of the state’s chief law enforcement official.  Mission: Our daily mission is to provide representation at the highest level to lawfully promote client policies and to ensure that Ohio businesses and residential customers enjoy reliable utility services at fair prices. | **Help Center**  Toll-free: 800-282-0515 Monday - Friday 8 a.m. - 6 p.m.  30 E. Broad St., 14th Floor Columbus, OH 43215  **BCI Tip Line**  Phone: 855-BCI-OHIO (855-224-6446)  Please be aware that the Attorney General's Office cannot provide legal assistance or advice to individuals. Information you receive from the Attorney General's Office is informal guidance.  It is not legal advice.  Any information provided to the Attorney General is considered a public record. |
| **Ohio State Auditor’s**  **Office** | Investigates criminal offenses affecting state resources, including computer security breaches. | Auditor of State  88 East Broad Street, 5th Floor Columbus, OH 43215  Public Line:  614-466-4514 | 800-282-0370  Legal Counsel: 800-282-0370  Fraud Hotline: 866-FRAUD-OH (866-372-8364) |
| **Ohio State Auditor’s**  **Office - Ransomware Notification Process** | Cyber Incident Response  What to do if infected with Ransomware  1. If you believe you are the victim of a ransomware attack, immediately remove the infected computer from your network and/or the Internet. This can be done by removing your network cable or turning off the computer’s WiFi connection. This will prevent the ransomware from attacking your network or share drives.  2. If you suspect other devices have been affected, you should isolate or power-off them as well. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.  3. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware. 4. We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) immediately to report a ransomware event and request assistance  5. Contact local law enforcement. Inform them that you have reported an incident to the FBI.  6. Contact your IT provider. Technical assistance will be needed to repair and restore your system.  7. Implement your business continuity plan while your system is being restored  [Cyber Incident Response.docx (ohioauditor.gov)](https://ohioauditor.gov/publications/docs/Cyber%20Incident%20Response.pdf) | Ohio FBI Field offices  Cincinnati Office for Southern counties  2012 Ronald Reagan Drive Cincinnati, OH 45236 cincinnati.fbi.gov  (513) 421-4310  Cleveland Office for Northern counties  1501 Lakeside Avenue  Cleveland, OH 44114  (216) 522-1400  If a non-infected system is available, a cyber incident can be reported at the following FBI  website: http://www.ic3.gov |
| **Ohio Emergency Management Agency** | Coordinates the state emergency management program and manages the Statewide Operations Center (SOC), which monitors threats, makes notification of threats, and provides information on emergency incidents to local, state, and federal officials. | 2855 West Dublin-Granville Road Columbus, Ohio 43235-2712 Phone: (614) 889-7150 General Fax: (614) 889-7183 |
| **County EMA Director** | Point of Contact to receive State of Ohio assistance for Ohio Critical Infrastructure. | [County] EMA Director  [First and Last Name]  [Phone]  [Email] |

#### Table 9.2: Federal Contacts

|  |  |  |
| --- | --- | --- |
| **Resource** | **Services** | **Contact Information** |
| **Federal Bureau of Investigation** | Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information. | Ohio FBI Field offices  Cincinnati Office for Southern counties  2012 Ronald Reagan Drive Cincinnati, OH 45236 cincinnati.fbi.gov  (513) 421-4310  Cleveland Office for Northern counties  1501 Lakeside Avenue  Cleveland, OH 44114  (216) 522-1400  If a non-infected system is available, a cyber incident can be reported at the following FBI  website: http://www.ic3.gov |
| **Federal Emergency**  **Management**  **Agency (FEMA)** | Provides disaster response and recovery assistance. | 1-800-621-FEMA (3362) |
| **National Cyber**  **Security Division**  **(NCSD), US Dept. of**  **Homeland Security** | Works collaboratively with public, private, and international entities to secure cyberspace and America’s cyber assets. | Response coordination: (202) 282-8000 |

|  |  |  |
| --- | --- | --- |
| **CERT Coordination Center (CERT/CC)** | Federally-funded CERT provide technical  advice to federal, state, and local agencies on responses to security compromises. | CERT 24-hour hotline: (412) 268-7090 forensics@cert.org |
| **US Secret Service** | Investigates financial crimes, including identity theft. | Austin Field Office: (512) 916-5103 |
| **US Treasury Inspector General for Tax**  **Administration (TIGTA) and Office of Safeguards** | Works with agencies to ensure that all appropriate actions are taken with regard to Federal Tax Information. | TIGTA Field Division, Dallas: (972) 308-1400 |
| **Federal Trade**  **Commission (FTC)** | Regulates consumer business practices. | <http://www.ftc.gov>Detecting identity theft: <http://www.ftc.gov/idtheft> |
| **National Institute of**  **Standards and**  **Technology (NIST),**  **US Dept. of**  **Commerce** | Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 (FISMA, 44 USC § 3541, *et seq.*). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government. | Main office: (301) 975-NIST inquiries@NIST.gov<http://www.nist.gov/index.html>    Publications: <http://csrc.nist.gov/publications/> |
| **Office for Civil**  **Rights (OCR), US**  **Dept. of Health and**  **Human Services** | Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA. | [http://www.hhs.gov/ocr/office/in dex.html](http://www.hhs.gov/ocr/office/index.html) |
| **US Postal Service**  **Inspector Service** | The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees. | [https://postalinspectors.uspis.gov](https://postalinspectors.uspis.gov/) |

#### Table 9.3: Industry Contacts

|  |  |  |
| --- | --- | --- |
| **Resource** | **Services** | **Contact Information** |
| **Ponemon Institute** | Conducts independent research on privacy, data protection, and information security policy. | [http://www.ponemon.org/index.](http://www.ponemon.org/index.php)  [php](http://www.ponemon.org/index.php) |
| **Credit Bureaus** | Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes. Consumers may request a 90-day or 7- year fraud alerts be attached to their credit bureau files by contacting one credit bureau which will in turn notify other bureaus. A credit freeze must be requested from each bureau. | Equifax:  P.O. Box 740241  Atlanta, GA 30374  Fraud Hotline (toll-free):  1-877-478-7625 [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com/)  Experian  P.O. Box 2002  Allen, TX 75013  Fraud Hotline (toll-free):  1-888-397-3742 [www.experian.com](http://www.experian.com/)  TransUnion  P.O. Box 6790  Fullerton, CA 92834  Fraud Hotline (toll-free):  1-800-680-7289 [www.transunion.com](http://www.transunion.com/)  Email to report suspected fraud: fvad@transunion.com  Annual Credit Report Request  Service  P.O. Box 105281  Atlanta, GA 30348-5281 1-877-322-8228 <http://www.ftc.gov/freereports>[www.AnnualCreditReport.com](http://www.annualcreditreport.com/) |
| **American Health**  **Information**  **Management**  **Association**  **(AHIMA)** | AHIMA is an association of health information management professionals with a useful resources page for health data. | [http://www.ahima.org/resources /infocenter/psc.aspx](http://www.ahima.org/resources/infocenter/psc.aspx) |
| **Health Information**  **Management**  **Systems Society**  **(HIMSS)** | HIMSS is an association of health information management professionals with resources page for health data. | [http://www.himss.org/ResourceLi brary/ResourceDetail.aspx?ItemN umber=17266](http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266) |
| **Payment Card**  **Industry – Data**  **Security Standards**  **(PCI-DSS)** | Payment card data security standards set by the payment card industry. | [https://www.pcisecuritystandards .org/security\_standards/](https://www.pcisecuritystandards.org/security_standards/) |

#### Table 9.4: Press Contacts

|  |  |  |
| --- | --- | --- |
| **Resource** | **Services** | **Contact Information** |
| **Ohio Press Contacts** | Ohio Media Directory (subscription for distribution lists for other cities and counties). | [Contact Ohio News Media at EasyMediaList.com](https://www.easymedialist.com/usa/state/ohio.html) |

### SECTION 10 Legal References

This section covers a list of federal and state laws establishing relevant standards for types of confidential data, including a brief summary and a citation. The list is not comprehensive; please refer to legal counsel for other relevant laws.

#### 10.1 Ohio Laws and Regulations for Data Privacy and Security.

None. Update as appropriate.

#### 10.2 Federal Laws and Regulations for Data Privacy and Security

|  |  |  |
| --- | --- | --- |
| **Health Insurance Portability and Accountability**  **Act (HIPAA) (1996)** | HIPAA contains the following provisions regulating the use and disclosure of protected health information:   * *Privacy Rule* protects the privacy of individually identifiable health information; * *Security Rule sets national standards for the security of electronic protected health information;* * *Breach Notification Rule requires covered entities and business associates to provide notification following a breach of unsecured protected health information;* * *Enforcement providing civil and criminal penalties for violation; and* * *Patient Safety Rule protects identifiable information being used to analyze patient safety events and improve patient safety.* | [HIPAA](https://www.govinfo.gov/app/details/PLAW-104publ191) |
| **Health**  **Information**  **Technology for**  **Economic and**  **Clinical Health**  **Act (HITECH)**  **(2009)** | HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA Business Associates and requiring Covered Entities and Business Associates to report data breaches to those affected individuals through specific breach notification requirements. | [HITECH (2009) (ARRA Title XIII)](http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf) |

|  |  |  |
| --- | --- | --- |
| **Federal**  **Information**  **Security**  **Management Act**  **(FISMA) (2014)** | Federal legislation that assigns specific responsibilities to federal agencies, the National Institute of Standards and  Technology (NIST), and the Office of Management and Budget (OMB) to provide for the strengthening of information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to effectively and efficiently drive down IT security issues to acceptable levels through a defined framework by which federal government agencies would ensure the security of information systems controlled by either the agency or one of its contractors on behalf of a federal agency. The framework is further defined by the standards and guidelines set forth by NIST. | [44 USC §§ 3541-](http://csrc.nist.gov/drivers/documents/FISMA-final.pdf)  [3549](http://csrc.nist.gov/drivers/documents/FISMA-final.pdf) |
| **Internal Revenue Service Statute and Regulation** | Through Publication 1075, the IRS has created a framework by which Federal Tax Information (FTI) and Personally Identifiable Information (PII) is protected from public disclosure. To ensure the safety of such data, receiving agencies and/or entities must have proper safeguards in place. Federal code requires external agencies and other authorized recipients of federal tax return and return information (FTI) to establish specific procedures to ensure the adequate protection of the FTI they receive. In addition, the same section of the Code authorizes the IRS to suspend or terminate FTI disclosure to a receiving agency or other authorized recipient if misuse or insufficient FTI safeguards are found. In addition to criminal sanctions, the Internal Revenue Code prescribes civil damages for unauthorized **disclosure** and, when appropriate, the notification to affected taxpayers that an unauthorized inspection or disclosure has occurred. | [Publication 1075;](http://www.irs.gov/pub/irs-pdf/p1075.pdf)  [IRC Section](http://www.law.cornell.edu/uscode/text/26/6103)  [6103(p)(4)](http://www.law.cornell.edu/uscode/text/26/6103); [26 USC](http://www.law.cornell.edu/uscode/text/26/6103)  [§6103(p)(4)](http://www.law.cornell.edu/uscode/text/26/6103) |
| **Social Security**  **Administration (SSA) Statute and Regulation** | Much of the information SSA collects and maintains on individuals is especially sensitive, therefore prior to disclosing such information, SSA must look to the Privacy Act of 1974, 5 USC Section 552a, FOIA, 5 **USC** Section 1106 of SSA, 42 USC Section 1306. SSA employees are prohibited from disclosing any information contained in SSA records unless disclosure is authorized by regulation or otherwise required by federal law. SSA may only disclose personal records (PII) when the individual to whom the record pertains provides written consent or when such disclosure falls into one of the several narrowly drawn exceptions. | [Privacy Act of](http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf)  [1974;](http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf)  [5 USC Section](http://www.law.cornell.edu/uscode/text/5/552a)  [552a;](http://www.law.cornell.edu/uscode/text/5/552a)  [FOIA;](http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm)  [5 USC §1106 (SSA);](http://www.socialsecurity.gov/OP_Home/ssact/title11/1106.htm)  [42 USC §1306](http://www.gpo.gov/fdsys/granule/USCODE-2010-title42/USCODE-2010-title42-chap7-subchapXI-partA-sec1306/content-detail.html) |
| **National**  **Institute of**  **Standards and**  **Technology**  **(NIST)** | NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and to help with managing cost effective programs to protect their information **systems** and the data stored on the systems. NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in FIPS 200. The security rule covers 17 areas, including control, incident response, business continuity, and disaster recoverability. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls. Agencies are expected to comply with NIST security standards and guidelines. | [NIST 800](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)[-](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)[53 rev. 5](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)[;](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)  [FIPS 200](http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf) |
| **Criminal Justice**  **Information**  **Services (CJIS)** | CJIS is a division of the FBI that compiles data provided by law enforcement agencies across the United States. CJIS is the world’s largest repository of criminal fingerprints and history records which can be accessed and searched by law enforcement to enable the quick apprehension of criminals.  The responsibility of CJIS extends to the Integrated  Automated Fingerprint Identification System (IAFIS), the  National Crime Information Center (NCIC), and the National Incident-Based Reporting System (NIBRS). In addition to its many responsibilities in the coordination and sharing of criminal data, CJIS promulgates the CJIS Security Policy, which is meant to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI). The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. The policy applies to every individual – contractor, private entity, noncriminal justice agency representatives, or members of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information. | [CJIS Security](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)  [Policy,](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)  [TGC § 552.108](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.108) |
| **Clinical**  **Laboratory**  **Improvements**  **Amendments**  **(CLIA)** | CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services. | CLIA Regulations and Guidance |
| **Computer Fraud and Abuse Act**  **(CFAA)** | CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines “protected computers” as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication. | [18 USC §1030](http://www.law.cornell.edu/uscode/text/18/1030) |

#### 10.3 Other Laws and Regulations for Data Privacy and Security

|  |  |  |
| --- | --- | --- |
| **General Data**  **Protection**  **Regulation**  **(GDPR)**  **(2018)** | The General Data Protection Regulation (GDPR) is a privacy and security law drafted and passed by the European Union (EU). It imposes obligations onto organizations across the globe, so long as they target or collect data related to people in the EU.  The GDPR includes many key regulatory points, including:   * Data protection principles * Accountability * Data security * Data protection by design and by default * When you’re allowed to process data * Consent * Data Protection Officers * Privacy rights | [**GDPR (**2018)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679) |

### Acknowledgements