Santa Maria ISD
Cybersecurity Annex

2024-2025

Cyber Incident Response Plan

NOTE: The *Cybersecurity Annex* works in conjunction with the *Cyber Incident Response Plan*. The Response Phase and Recovery Phase (also known as During a Cybersecurity Incident and After a Cybersecurity Incident) are outlined in depth in the *Cyber Incident Response Plan*.

SPECIAL ACKNOWLEDGEMENTS

The Texas School Safety Center is grateful for the contributions of the specialists in directing the subject matter knowledge for this annex. We appreciate your help in creating this template, which is for use by colleges and K-12 districts throughout the state. Your knowledge was invaluable in creating this template and subsequent completion guide.

A special thank you goes to:

Todd Pauley, CISSP, CISM
Deputy CISO and Cybersecurity Coordinator, Texas Education Agency

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas, Cybersecurity, and Infrastructure Security Agency

Tony Sauerhoff, CISSP, GSLC
Deputy CISO and State Cybersecurity Coordinator, Texas Department of Information Resources

RECORD OF CHANGES AND REVIEW

The Cybersecurity Annex will be reviewed periodically, *but no less than every three years*, and be properly coordinated with the district's other plans.

The Cybersecurity Annex's notable modifications are included in the table along with the date of the Annex's review. Add additional rows as needed.

This Record of Changes and Review identifies only significant changes made to this Annex. If no significant changes were made, the phrase "Cybersecurity Review Conducted" has been placed in the *Summary of Significant Changes and Review* column.

Change Number	Date of Change	Name of Person or Agency Making the Change	Summary of Significant Changes and Review
1	2021	Doralee Rivera-Munoz	Technology Coordinator Arturo Hinojosa, Jr. has been added to the plan.
2	2024	Doralee Rivera-Munoz	Replace former Superintendent Martin Cuellar to new Superintendent Dr. Joseph Villarreal

© TxSSC, 2024

Section 1 – Purpose and Scope

1.1 Purpose

This annex establishes the policies and procedures under which the district will operate in the event of a cybersecurity incident by addressing planning and operational actions for the five phases of emergency management (prevention, mitigation, preparedness, response, and recovery) regarding actual or potential cyber-related threats and attacks to the district.

1.2 Scope

This annex is meant to address district planning for cybersecurity incidents and applies to the whole district community and all district property.

© TxSSC, 2024

Section 2 – General Information

2.1 Hazard Overview

Cybersecurity establishes the measures taken to protect a computer, computer network, or computer system against unauthorized use or access, otherwise known as a cyber incident. According to the Presidential Policy Directive (PPD) 41, a cyber incident is

> "An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."

A cyber incident could affect building access, phone systems, security systems, learning management systems, human resources, payroll, student records, school nutrition services, visitor management systems, printing services, library services, staff information, and other systems that use a computer network.

2.2 District-Specific Hazard Risk

Santa Maria ISD notes the level of risk concerning cybersecurity incidents using a *Cybersecurity Risk Evaluation Tool*.

Santa Maria ISD identifies the following cyber incidents as a high priority. If needed, these hazards are addressed in an appendix to this annex.

Breach of security system

A breach of security system occurs when private, sensitive, or protected information is spilled or leaked from a safe setting into an unsecured one, where it is subsequently seen, copied, communicated, stolen, or used without authorization. Confidential information, like student records, is frequently the subject of data breaches because it might be improperly seen or used by someone who should not have access.

Denial of Service attacks (DOS and DDoS)

A Denial of Service (DOS) attack occurs when hackers use false requests and traffic to overwhelm a system and shut it down. A Distributed Denial of Service (DDoS) attack is the same type of attack, except the hacker uses multiple breached devices at the same time.

Fraudulent Instruction

Fraudulent Instruction usually occurs as a targeted phone call or email that convinces an employee to alter the direct deposit information for a worker, or more seriously, for a district-funded building project.

Malware-based attacks (Ransomware, Trojans, etc.)

Malware refers to "malicious software" that is designed to disrupt or steal data from a computer, network, or server.

© TxSSC, 2024

Man-in-the-Middle (MitM)
A Man-in-the-Middle attack (MitM) occurs when attackers intercept data or compromise your network to “eavesdrop” on you. These attacks are especially common when using public Wi-Fi networks, which can easily be hacked.

Password attacks
Password attacks are any cyberattack that uses brute force, guesswork, or deception to get you to divulge your passwords.

Phishing (spear phishing, whaling, etc.)
A phishing attack occurs when a cybercriminal sends you a fraudulent email, text (called “smishing”), or phone call (called “vishing”). These messages look like they are from someone official or a person or business whom you trust, such as your bank, the FBI, or a company like Microsoft, Apple, or Netflix.

Ransomware
Malevolent software that locks user access by encrypting data while extorting payment (a “ransom”) from the victim to de-encrypt and restore the files.

Spoofing
Email messages sent from a fraudulent account masquerading as a legitimate and trusted source to gain access to a user’s system or confidential information.

Spyware
Criminal malware on the hard drive is used to covertly monitor user activities.

Virus
A type of malware that when executed spreads from computer to computer by replicating its programming and infecting user programs and files to change the way they operate or to stop working altogether.

Zero-day exploits and attacks
Zero-day exploits are cybersecurity vulnerabilities that exist in software or network without the manufacturer’s knowledge.

2.3 Hazard Preparedness and Warning
Santa Maria ISD has committed to being prepared for high-priority incidents as identified in the *District-Specific Hazard Risk* (section 2.2). The following are steps that the district will take to prepare for an incident.

Backup Data
Employ a backup solution that automatically and continuously backs up critical data and system configurations. Backup files are either stored in the cloud or if backed up to a local, portable drive, maintained off the network for secure storage. If the backups are stored off-site, but still on the network, they would still be susceptible to an attack.

© TxSSC, 2024

The district recognizes that if backup files are stored in the same place where the primary files are stored, then there is a high probability that in an incident, both sets will be destroyed.

Multi-Factor Authentication (MFA)

Require Multi-Factor Authentication (MFA) for accessing systems as needed. MFA is required with privileged, administrative, and remote access users, and will eventually be required by all users.

Patch and Update Management

Replace unsupported operating systems, applications, and hardware. Test and deploy patches quickly.

Suspicious Activity

Watch for suspicious activity that asks a user to do something right away, offers something that sounds too good to be true, or requests personal information.

Inadvertent Loss to Environmental Factors

Servers and other critical network infrastructure are not in rooms subject to water leaks (overhead plumbing) or accidental sprinkler damage. Additionally, adequate air conditioning is maintained in rooms in which network equipment is used.

© TxSSC, 2024

Section 3 – Cyber Incident Stakeholders

3.1 Cyber Incident Stakeholders Chart

Santa Maria ISD has listed all stakeholders and decision-makers during a cyber incident.
**The list of individuals below is provided for informative reasons and does not indicate the order or necessity to be called for every situation.*

Contact Role	Contact Name	Phone Number	Email
Superintendent	Dr. Joseph Villarreal	956-565-6308	idatorres@smisd.net
District Project Manager	Doralee Munoz	956-565-6308	doraleemunoz@smisd.net
Federal Programs Director	Salvador Acosta	956-565-6308	sacosta@smisd.net
Human Resource Specialist	Elizabeth Stenhouse	956-565-6308	elizabethstenhouse@smisd.net
Campus Principal(s)	Yadira Flores	956-565-9144	yadiraflores@smisd.net
Campus Principal(s)	Jay Viera	956-565-6309	jayviera@smisd.net
Campus Principal(s)	Jacob Camacho	956-565-5348	jacobcamacho@smisd.net
Technology/Cybersecurity Coordinator	Arturo Hinojosa, Jr.	956-565-6308	arturohinojosajr@smisd.net
Legal Counsel	O'Hanlan Group	956-565-6308	hr@smisd.net
Critical Vendor	Insight Public Sector Gabriel Sagrado	956-	gabriel.sagrado@insight.com
Education Service Center One-Technology Director	Daniel Ramirez	956-984-6061	danramirez@esc1.net
FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov	San Antonio Field Office - Cyber	210-225-6741	210-225-6741
Department of Homeland Security - CISA https://www.cisa.gov/report	Harvey Perriott CISA Region 6	888-282-0870	cisaregion6@cisa.dhs.gov
Texas Dept. of Information Resources (DIR) Management and Reporting	Nancy Rainosek (Texas State CISO)	877-347-2476	cirt@dir.texas.gov
State, County, or Local Government Liaison(s)	Juanita Jaimez	956-797-1887	
Texas Education Agency	Melinda Dade (TEA CISO)		cybersecurity@tea.texas.gov
Police	Baudelio Castillo	956-565-6309	bcastillo@smisd.net
Police	City of La Feria Police Department-Cesar Diaz	956-797-3121	cdiaz@cityoflaferia.com
ISP-Orion	Smartcom Telephone, LLC.	956-213-2010	repairs@sctel.co
ISP-Smartcom	Smartcom Telephone, LLC.	956-213-2010	repairs@sctel.co

© TxSSC, 2024

3.2 Build a Cyber Incident Response Team and Define the Roles

Santa Maria ISD has defined roles for the execution and management during a cyber incident.

Role	Responsibilities	Contact Name	Phone Number	Email
Cyber Incident Response Team Lead	Manage incident operations Identify and apply resources	Arturo Hinojosa, Jr.	956-565-6308	Arturohinojosajr@smisd.net
Team Administrator	Document incident Compile data Contact list Distribution Point of Contact for outside agencies	Chief Baudelio Castillo	956-565-6309	bcastillo@smisd.net
Team Lead Investigator	Coordinate response activities Technical aspects	Chief Baudelio Castillo	956-565-6309	bcastillo@smisd.net
First Responder	Investigation Reporting Arrest	Chief Baudelio Castillo	956-565-6309	bcastillo@smisd.net
Public Relations	Contact List All inbound and outbound communication	Chief Baudelio Castillo	956-565-6309	bcastillo@smisd.net
Federal Government Liaison	Contact list Request resources National reporting and tracking system of cybersecurity incidents	Arturo Hinojosa, Jr.	956-565-6308	Arturohinojosajr@smisd.net
Superintendent	Inform required stakeholders	Dr. Joseph Villarreal	956-565-6308	idatorres@smisd.net

© TxSSC, 2024

Section 4 – Actions and Responsibilities

District Actions and Responsibilities Table

Responsible Role refers to a ***single*** responsible role associated with the district action. This individual will oversee the action's completion and any necessary general training. However, this individual may not be the same as the individual or individuals that perform the action.

Prevention Phase **Safeguard against consequences unique to a cybersecurity incident.**	
District Actions	Responsible Role (Position responsible for this action)
Designate a District Cybersecurity Coordinator to serve as a liaison between the district and the agency in cybersecurity matters.	Superintendent
Complete state certified annual training for the District Cybersecurity Coordinator located on the DIR website, per Texas Education Code §11.175(h-1). DIR Statewide Cybersecurity Awareness Training	Cybersecurity Coordinator, **September 30, 2024**
Conduct a risk assessment of cybersecurity threats and vulnerabilities. • Identify the attractiveness of potential targets. • Identify critical district processes and assets.	Technology Coordinator
Install host-based firewalls and Endpoint Detection and Response (EDR) software security products.	Technology Coordinator
Configure network firewalls to block unauthorized IP addresses.	Technology Coordinator
Install EDR software.	Technology Coordinator
Employ a backup solution that automatically and continuously backs up critical data and system configurations.	Technology Coordinator
Regularly test the restoration of data.	Technology Coordinator
Disable port forwarding (disable the ability to connect over the internet with other public or private computers).	Technology Coordinator
Sign up for Dorkbot web application vulnerability notification service.	Technology Coordinator
Prepare a contact list of roles for the execution and management (*Section 3.2: Build a Cyber Incident Response Team and Define the Roles*) during a security incident and disseminate it to relevant parties.	District Project Manager

© TxSSC, 2024

Mitigation Phase

Reduce the impact of a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Conduct continuous vulnerability scans on Santa Maria ISD owned systems.	Technology Coordinator
Provide updates on LEA owned systems, including all internet connected devices (i.e., smartphones and tablets), whenever possible. Replace unsupported operating systems, applications, and hardware. Consider testing a small percentage of systems before patching all systems.	Technology Coordinator
Set EDR and anti-malware solutions to automatically update and conduct regular scans.	Technology Coordinator
Separate student networks from other sensitive district networks where possible.	Technology Coordinator
Apply the Principle of Least Privilege (PoLP) for employees to all LEA owned systems and services so that users only have the access they need to perform their jobs.	Technology Coordinator
Highly recommend the use of Multi-Factor Authentication (MFA) for accessing critical systems and consider using for all systems.	Technology Coordinator
Enable the most secure authentication tools available, such as biometrics, security keys, or a unique one-time code through an app on the mobile device.	Technology Coordinator
Close or block network ports that are not in use to reduce the threat landscape of potential attacks.	Technology Coordinator

© TxSSC, 2024

Preparedness Phase

Regularly review district readiness for a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Create an annual training plan for all employees and students.	Technology Coordinator
Train faculty and staff on cybersecurity incidents annually.	Technology Coordinator
Train students on cybersecurity incidents annually.	Principal
Conduct cybersecurity training for Board Members.	Technology Coordinator
Join an information sharing program through ESC.	Technology Coordinator
Document information flows by learning where data is located and how it is used for the district.	Technology Coordinator
Maintain hardware and software inventory.	Technology Coordinator
Ensure proper audit logs are created and reviewed routinely for suspicious activity.	Technology Coordinator
Monitor privacy settings and information available on social networking sites.	Technology Coordinator
Test and update response plans by conducting tabletop exercises.	Chief of Police
Perform annual penetration testing and routine vulnerability assessments.	Technology Coordinator
Ensure all students and employees understand and sign a network use agreement that explicitly outlines bad behaviors and consequences.	Technology Coordinator
Develop business continuity plans, as part of your Continuity of Operations Plan (COOP), for each department with essential functions.	District Project Manager
Establish an Interagency Contract with the Department of Information Resources (DIR).	Technology Coordinator
Consider purchasing cyber insurance for the district.	Superintendent
Learn what actions to avoid that could disrupt the insurance process	Superintendent

© TxSSC, 2024

Response Phase

District actions during a cybersecurity incident.

Refer to ***Section 5 - Document 4: Cyber Incident Response Plan*** when a cyber incident occurs. This plan is specific to cyber incidents and clarifies roles and responsibilities as well as provides guidance on key activities that must be performed. This plan must be carried out quickly so make sure to practice it before an actual incident occurs. This plan helps prevent data and monetary loss and to resume normal operations.

The Cyber Incident Response Plan is attached to the back of this annex due to the need to access the steps quickly and easily.

Recovery Phase

Return to normal district operations following a cybersecurity incident.

Refer to ***Section 5 - Document 4: Cyber Incident Response Plan*** for the recovery phase. The plan specifies steps to help resume normal operations.

© TxSSC, 2024

Section 5.0 - Documents

Document 1: Anomalies Report *(optional)*

Reporting System for Anomalies

It is important to report computer anomalies, system performance issues, strange defects in operation, etc. to the school IT Director or division. Early warning signs of Indication of Compromise (IoC), reported early, can prevent possible cascading outages. Staff should be encouraged and empowered to report such system behaviors.

When reporting attempt to provide the following:

Anomalies Reporting Table

Point of Contact	**Name**	**Email**	**Phone Number**
	Arturo Hinojosa, Jr.	Arturohinojosajr@smisd.net	956-565-6308
Date of Indication of Compromise	None	**Time of Indication of Compromise**	None
Manufacturer	NA	**Operating System (OS)**	NA
Description of Behavior	N/A		

© TxSSC, 2024

Document 2: Services Restoration Priority Worksheet *(optional)*

This restoration worksheet identifies the services and systems used the district to conduct its internal and external operations. Prioritization of services and systems are critical to support restoration priorities during incident response and recovery activities. These may be listed and prioritized as part of the business continuity or disaster recovery planning process.

Consider the restoration priority for your district using the following classifications:

- *Tier 1:* Critical services or systems and life safety or public safety systems.
- *Tier 2:* Core business functions and services that enable district operations.
- *Tier 3:* Routine business functions and services that support district operations.
- *Tier 4:* Non-production services or functions that do not impact the end users.

Tier	Service or System	Function and Details	End User
Ex. 3	*Library*	*Loaning and receiving multimedia, iPad registration and insurance*	*Students*
1	Upon Request		
	(Optional)		
2			
3			
4			

{Excerpt from "Services Restoration Priority Worksheet" by DIR is licensed under CC BY 4.0}

Document 3: Hardware and Software Inventory *(optional)*

It is highly encouraged to track the district's IT resources, including computers, servers, mobile devices, IP phones, other internet-connected devices, and approved and managed software. This inventory allows IT or your managed service provider to track devices to maintain and provides a starting point to prioritize disaster recovery efforts.

Hardware Tracking Inventory

Complete and maintain the following hardware asset tracking sheet. Customize the headers as appropriate.

Asset Number	Current Status	Assigned Employee	Asset Type	Model	Manufacture	Serial Number	Location	Description	Date Issued	Date Returned
Upon	Request	(optional)								

Software Tracking Inventory

Complete and maintain the following software tracking sheet. Customize the headers as appropriate.

Software User	Name	Software Description	License Type	Version	Software Key	Date Purchased	Billing Cycle

Sensitive Asset Inventory

Complete and maintain the following sensitive asset tracking sheet. Customize the headers as appropriate.

File Name	File Type	Description	Type of Storage	Data Storage Location	Data Classification Label	Reason for Sensitivity	Individuals with Access	Notes

{Excerpt from "CIS Hardware and Software Asset Tracking Spreadsheet" by CIS Controls™ is licensed under CC BY 4.0}

Document 4: Cyber Incident Response Plan (IRP)

Before a Cybersecurity Incident

Refer to *Section 4 – Actions and Responsibilities* for the Prevention, Mitigation, and Preparation Phases to prepare before a cybersecurity incident occurs.

During a Cybersecurity Incident

District actions during a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Contact the IT director or team lead through established channels, as well as communication channels that do not use the ISD network (i.e., cell phones, Gmail, etc.).	Chief of Police
When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.	Technology Coordinator
Determine the appropriate power-down option. Consider disconnecting from the network rather than shutdown. Forensic data can be destroyed if the operating system (OS) executes a normal shutdown process.	Technology Coordinator
Block compromised systems from communicating with other devices or with attackers.	Technology Coordinator
Seek legal guidance ***before*** initiating communications.	Superintendent
Contact a cyber insurance provider or broker if the district has an existing policy.	Technology Coordinator
Contact all critical software vendor(s).	Technology Coordinator
Contact the FBI, Law Enforcement, and Homeland Security, as needed.	Chief of Police
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week Districts must report security incidents to DIR within 48 hours after discovery per Texas Government Code, Section 2054.603.	Technology Coordinator
Consult with trained forensic investigators for advice and assistance ***prior*** to implementing any recovery or forensic efforts.	Chief of Police
Contact banks, credit card companies, and other financial accounts to report that someone may be using the district's identity. Holds may need to be placed on accounts that have been attacked. Unauthorized credit or charge accounts will need to be closed.	Federal Programs Director

© TxSSC, 2024

During a Cybersecurity Incident

District actions during a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Keep detailed notes of all observations, including dates and times, mitigation steps taken and not taken, device logging enabled or disabled, and machine names for suspected compromised equipment. More information is generally better than less information.	Technology Coordinator
Oversee and track containment and restoration activities, including actions taken, resource assignments, and notifications.	Superintendent
Initiate Continuity of Operations Plan (COOP) and essential department continuity plans.	District Project Manager
Track hazard-related expenses.	Federal Programs Director

After a Cybersecurity Incident

Return to normal district operations following a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Ensure that personnel are made available to provide statements to law enforcement and other investigating authorities.	Chief of Police
Conduct a root cause analysis to pinpoint where a malicious incident took place.	Technology Coordinator
Communicate with internal and external stakeholders and manage public relations and reputation, including parents of students, if necessary.	Superintendent
Conduct continuous monitoring of networks after a breach for any abnormal activity and make sure intruders have been inhibited thoroughly.	Technology Coordinator

© TxSSC, 2024

After a Cybersecurity Incident

Return to normal district operations following a cybersecurity incident.

District Actions	Responsible Role (Position responsible for this action)
Activate the damage assessment team.	District Project Manager
Work with affected system and service owners and managers to determine resources and sequencing needed to restore operations to a normal state.	Technology Coordinator
Based on priorities and estimated recovery timelines, repair, restore, rebuild, or replace systems that were taken offline or otherwise affected by the incident after they are cleared and released by investigators.	Technology Coordinator
Track restoration efforts and provide information to the emergency management team (EMT) regarding estimated and actual time to full restoration.	Technology Coordinator
After ensuring evidence has been preserved for legal and insurance purposes, and given the all-clear, eliminate all traces of the incident.	Technology Coordinator
Track damages and expenses for reimbursement claims.	Federal Programs Director
Conduct an After-Action Review (AAR) to identify areas of improvement for the incident response plan.	District Project Manager
Develop and implement an Improvement Plan (IP) that includes recommended changes from the incident debriefing and AAR.	District Project Manager
Share lessons learned through appropriate channels.	Technology Coordinator
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week at (877) 347-2476 (877-DIR-CISO). Districts must report security incidents to DIR within 10 days of incident closure per Texas Government, Code Section 2054.603.	Technology Coordinator
Districts must notify any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person no later than the 60th day after the date on which the breach was determined to occur per Texas Government Code section 2054.603.	Human Resource Specialist

© TxSSC, 2024

Section 6 – Resources

6.1 Abbreviations and Acronyms

AAR	After-Action Review
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
DIR	Department of Information Resources
DDoS	Distributed Denial of Service
DOS	Denial of Service
EDR	Endpoint Detection and Response
EMT	Emergency Management Team
IAM	Identity and Access Management
Infosec	Information Security
IoC	Indication of Compromise
IT	Information Technology
K12 SIX	K12 Security Information eXchange
LEA	Local Education Agency
LOA	Letters of Agreement
MFA	Multifactor Authentication
MitM	Man-in-the-Middle
MOU	Memoranda of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
OIG	Office of the Inspector General
OS	Operating System
PII	Personal Identifying Information
PoLP	Principle of Least Privilege
SSO	Single Sign-On
TASB	Texas Association of School Boards
TEC	Texas Education Code
TGC	Texas Government Code
TX-ISAO	Texas Information Sharing and Analysis Organization
URL	Uniform Resource Locator

6.2 Definitions

Antivirus Software: Responsible for scanning your files and looking for viruses. While it is often marketed as an antivirus, most antivirus software is anti-malware even though it's frequently promoted as antivirus (Ot, 2021).

Authentication: A security measure employed to confirm the identity of the person making a request or the message's originator when trying to authorize access to data or computer resources.

Brute Force Attack: A hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

© TxSSC, 2024

Bug: An error, flaw, or fault in the design, development, or operation of computer software.

Cyberattack: Attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity: Measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Cyber Resilience: The capacity to foresee, endure, recover from, and adapt to unfavorable circumstances, stressors, attacks, or compromises on systems that use or enable cyber resources.

Domain Spoofing: The act of registering web domains like legitimate websites to trick individuals who mistype URLs or click on similar-looking URLs.

Doxing: The act of compiling or publishing personal information about an individual on the internet, typically with malicious intent.

Endpoint: Physical devices that connect to a network system such as mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Endpoint Security: is security to protect desktops, laptops, mobile phones, etc. from malicious, unwanted software.

End of Life Software: Out-of-date software and equipment that no longer receives patches, security updates, technical support, or bug fixes, making the user vulnerable to attacks.

Firewalls: Software program or hardware device that restricts communication between a private network or computer system and outside networks.

Information Security: Protection of information and information systems from unauthorized access and disruption.

Information Technology: Development, installation, and implementation of computer systems and applications.

Malicious Cyber Actor: A person, group, or entity that creates all or part of an incident with the aim to impact an individual’s or organization’s security.

Malware-based Attacks: Malware refers to “malicious software” that is designed to disrupt or steal data from a computer, network, or server.

Multifactor Authentication: Security technology that requires multiple methods of authentication from independent categories of credentials to verify a user’s identity (such as a password and a code or fingerprint).

Patch: A software update that can be installed to correct an issue or fix security vulnerabilities.

© TxSSC, 2024

Port Forwarding: Allows computers or services in private networks to connect over the internet with other public or private computers or services, sometimes called port mapping.

Root Cause Analysis: Investigates the core issue that kicks off a chain of events that eventually results in the problem. It also looks for a solution in such a way that the problem is treated at the "root" or fundamental cause of the issue.

Texas Education Code § 11.175(b): District Cybersecurity Each school district shall adopt a cybersecurity policy to: (1) secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents; and (2) determine cybersecurity risk and implement mitigation planning.

6.3 Resources

Cyber Insurance Information

Ritchie, J.N.& A. and Jayanti, S.F.-T., and A. (2021) *What should your cyber insurance policy cover? Cyber Insurance*, *Federal Trade Commission*. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance (Accessed: 06 October 2023).

Explains why a cyber insurance policy is useful and what the policy should cover.

Cybersecurity Risk Assessment Tools

CISA. (n.d.). Guide to Getting Started with a Cybersecurity Risk Assessment. SAFECOM. Available at: https://www.cisa.gov/sites/default/files/2024-01/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508.pdf

This handbook was created by SAFECOM to help public safety communications system operators, owners, and managers comprehend the processes of a cyber risk assessment to increase operational and cyber resilience. This manual contains editable reference tables that can be used by districts to identify and record the people and resources used at each stage of the assessment. Customization is encouraged.

DIR. (n.d.). *Texas Cybersecurity Framework | Texas Department of Information Resources*. Information Security. https://dir.texas.gov/information-security/security-policy-and-planning/texas-cybersecurity-framework

The Texas Cybersecurity Framework is a self-assessment to determine cybersecurity risks. This sample is populated with examples of how to rate yourself based on the 6 levels identified at the bottom of the first tab (SAMPLE TCF). Once you have rated yourself in all 40 objectives the graph helps determine the highest risks and prioritization for mitigation. The roadmap will help identify processes and documentation needed to reach 3.0 in each objective.

Cybersecurity Plan Building Tools

© TxSSC, 2024

CISA. (2023, January). *Protecting our future: Cybersecurity for K-12: CISA*. Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats. https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Reports on cybersecurity risks facing elementary and secondary schools and provides recommendations that include cybersecurity guidelines designed to help schools face these risks.

Grants

DIR. (2023, October 6). *State and local cybersecurity grant program (SLCGP)*. Information Security. https://dir.texas.gov/information-security/state-and-local-cybersecurity-grant-program-slcgp

The State and Local Cybersecurity Grant Program (SLCGP) has been given $1 billion over four years (2022-2025) to address cybersecurity risks and threats to information systems owned or run by, or on behalf of, state, local, or tribal governments.

Easterly, J. (2023, October 18). *CISA and FEMA partner to provide $374.9 million in grants to bolster state and local cybersecurity: CISA*. Cybersecurity and Infrastructure Security Agency (CISA). https://www.cisa.gov/news-events/news/cisa-and-fema-partner-provide-3749-million-grants-bolster-state-and-local-cybersecurity

For access to FY23 funding, applicants are encouraged to submit their cybersecurity plans created with FY22 money. With this financing, the Department of Homeland Security strengthens our collaboration and commitment to assisting our state, local, and territorial (SLT) government partners in developing the necessary cyber capabilities.

© TxSSC, 2024

FEMA. (2023). *Tribal cybersecurity grant program*. Preparedness Grants. https://www.fema.gov/grants/preparedness/tribal-cybersecurity-grant-program

The Tribal Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of tribal governments.

FEMA. (2023). *State and local cybersecurity grant program*. Preparedness Grants. https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

TASB. (n.d.). *About TASB Risk Fund*. Risk Management Fund. https://www.tasbrmf.org/about?rname=RMF_Benefits_And_Rewards

The TASB Risk Management Fund provides comprehensive and responsive risk solutions supporting educational excellence in Texas public school districts and other public educational entities.

Texas Education Agency. (2023, September 21). *Tx K-12 Cybersecurity Initiative Updates*. TEA. https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/tx-k-12-cybersecurity-initiative-updates

LEAs who are interested and eligible to acquire TEA-funded Endpoint Detection and Response (EDR) may now request this service via the Service Now portal.

Information Sharing Tools

Cybersecurity & Infrastructure Security Agency. (2023). *Incident reporting system*. CISA. https://www.cisa.gov/forms/report

Provides real-time analysis and incident reporting capabilities.

Technical Assistance

Texas Education Agency. (2023, October 2). *K-12 cybersecurity initiative*. https://tea.texas.gov/academics/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

TEA in conjunction with DIR. Free Endpoint Detection & Response (EDR) subscriptions through the end of 2024-25 SY. Request for service is now open! Prioritized for small & midsize LEAs.

Texas Education Agency. (2023, November 30). *Standards for permissible electronic devices and software applications*. https://tea.texas.gov/about-tea/news-and-multimedia/correspondence/taa-letters/standards-for-permissible-electronic-devices-and-software-applications

House Bill 18 (88R) established Texas Education Code, Section §32.1021 and requires the TEA to provide these Standards for Electronic Devices and Software Applications with which school districts or open-enrollment charter schools are expected to comply.

© TxSSC, 2024