Temple College
Cybersecurity Annex

TEMPLE COLLEGE
Your Community's College

September 1, 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 college's other plans.

The table includes the Cybersecurity Annex's notable modifications and the date of its 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 and Title Making the Change	Summary of Significant Changes and Review
1	9/1/2024	Caleb Hogue, Chief Information Officer	Initial Plan for Adoption
2	9/1/2025	Caleb Hogue, Chief Information Officer	Annual Update, Updated contact information

Section 1 – Purpose and Scope

1.1 Purpose

This annex establishes the policies and procedures under which Temple College will operate in the event of a cybersecurity incident. It addresses 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 College.

1.2 Scope

This annex addresses Temple College's planning for cybersecurity incidents and applies to the whole college community and all college property.

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 computer network systems.

2.2 College-Specific Hazard Risk

Temple College notes the level of risk concerning cybersecurity incidents using a *Cybersecurity Risk Evaluation Tool*.

Temple College prioritizes the following cyber incidents. If needed, these hazards are addressed in an appendix to this annex.

Data Breach

A data breach 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 simultaneously.
Temple College utilizes DOS and DDoS protection through an external DNS hosting service and on both internal and external firewalls.

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 college-funded building project.
Temple College performs annual cybersecurity training sessions and quarterly simulations to help prevent Fraudulent Instruction.

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.
Temple College utilizes Endpoint Detection and Response (EDR) software on all college-owned machines to prevent malware-based attacks.

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.
Temple College utilizes encrypted VPN software to prevent MitM attacks in public spaces.

Password attacks

Password attacks are any cyberattack that uses brute force, guesswork, or deception to get you to divulge your passwords.
Temple College enforces a password policy and multi-factor authentication to prevent password-based attacks.

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.
Temple College utilizes email filtering with link sanitization and annual cybersecurity training to help prevent phishing attacks.

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.
Temple College utilizes Endpoint Detection and Response (EDR) software on all college-owned machines to prevent malware-based attacks.

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.
Temple College utilizes email filtering with anti-spoof detection to prevent spoofing attacks.

Spyware

Criminal malware on the hard drive is used to covertly monitor user activities.
Temple College utilizes Endpoint Detection and Response (EDR) software on all college-owned machines to prevent malware-based attacks.

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.
Temple College utilizes Endpoint Detection and Response (EDR) software on all college-owned machines to prevent malware-based attacks.

Zero-day exploits and attacks
Zero-day exploits are cybersecurity vulnerabilities that exist in software or network without the manufacturer's knowledge.
Temple College utilizes Endpoint Detection and Response (EDR) software on all college-owned machines to prevent malware-based attacks.

2.3 Hazard Preparedness and Warning
Temple College has committed to preparing for high-priority incidents identified in the *College-Specific Hazard Risk* (section 2.2). The college has taken the following steps to prepare for an incident.

Backup Data
Employ a backup solution that automatically and continuously backs up critical data and system configurations. Temple College uses a 3-2-1 Backup Strategy. Backup files are stored with copies at multiple geographical locations, and one offline copy is stored in a fireproof safe.

The college recognizes that if backup files are stored in the same place as the primary files, both sets will likely be destroyed in an incident.

Multi-Factor Authentication (MFA)
Require Multi-Factor Authentication (MFA) for accessing systems whenever possible. MFA is currently required for privileged, administrative, and remote access users and will eventually be required for all users.

Patch and Update Management
Replace unsupported operating systems, applications, and hardware. Test and deploy patches quickly.
Temple College utilizes an automated patch management solution to update operating systems 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 where network equipment is used.

Temple College has server infrastructure in multiple geographical locations to help prevent loss due to environmental factors.

Section 3 – Cyber Incident Stakeholders

3.1 Cyber Incident Stakeholders Chart

Temple College 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
Temple College President	Christy Ponce	254-298-8299	Christy.ponce@templejc.edu
Vice President of Administrative Services	Glenn Graham	254-298-8454	Glenn.graham@templejc.edu
Chief Information Officer	Caleb Hogue	254-298-8444	Caleb.hogue@templejc.edu
Chief Information Security Officer	John Greiner	254-298-8464	John.greiner@templejc.edu
Director of Network and Infrastructure Services	Cory Vahue	254-298-8458	Cory.vahue@templejc.edu
Director of IT Support	Ryan Brown	254-298-8430	Ryan.brown@templejc.edu
Director of ERP Services	James Ross	254-298-8445	James.ross@templejc.edu
Chief of Police	Stella Bergeron-Green	254-298-8910	Stella.bergeron-green@templejc.edu
Interim Director of Purchasing	Cienna McMurry	254-298-8608	Cienna.mcmurry@templejc.edu
Fortinet	Don Dodson	512-432-1355	ddodson@fortinet.com
FortiGuard Incident Response Services		1-866-868-3678	
Dell Account Manager	Scott Towel	512-840-8040	Scott.towel@dell.com
Cyber Insurance Broker or Provider AIG	Carrie Kurzon	(212) 458-2396	cyberlosscontrol@aig.com carrie.kurzon@aig.com
Texas Association of School Boards Cyber Insurance	Heide Gaden	(512) 505-2816	Heide.Gaden@tasb.org
Texas Department of Information Resources CISO		877-347-2476	cirt@dir.texas.gov
Department of Homeland Security - CISA https://www.cisa.gov/report			https://www.cisa.gov/report

State, County, or Local Government Liaison(s)	Adam Ward	254-933-5277	Adam.ward@bellcounty.texas.gov

3.2 Build a Cyber Incident Response Team and Define the Roles

Temple College has defined the roles of 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	Caleb Hogue, Chief Information Officer	254-298-8444	Caleb.hogue@templejc.edu
Team Administrator	Document incident Compile data Contact list Distribution Point of Contact for outside agencies	John Greiner Chief Information Security Officer	254-298-8464	John.greiner@templejc.edu
Team Lead Investigator	Coordinate response activities Technical aspects	Cory Vahue, Director of Network and Infrastructure Services	254-298-8458	Cory.vahue@templejc.edu
First Responder	Investigation Reporting Arrest	Stella Bergeron-Green, Chief of Police	254-298-8910	Stella.bergeron-green@templejc.edu
Public Relations	Contact List All inbound and outbound communication	Eric Eckert, Executive Director of Communications	254-298-8561	Eric.eckert@templejc.edu
Federal Government Liaison	Contact list Request resources National reporting and tracking system of cybersecurity incidents	Texas Department of Information Resources CISO	877-347-2476	cirt@dir.texas.gov

Section 4 – Actions and Responsibilities

College Actions and Responsibilities Table

Responsible Role refers to a ***single*** responsible role associated with the college's 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 who perform the action.

Prevention Phase **Safeguard against consequences unique to a cybersecurity incident.**	
College Actions	**Responsible Role (Position responsible for this action)**
Designate a cybersecurity coordinator to serve as a liaison between the college and the agency in cybersecurity matters.	Chief Information Security Officer
Conduct annual training for the College Cybersecurity Coordinator.	Chief Information Security Officer
Conduct a risk assessment of cybersecurity threats and vulnerabilities. • Identify the attractiveness of potential targets. • Identify critical college processes and assets.	Chief Information Security Officer
Install host-based firewalls and endpoint security products.	Director of Network and Infrastructure Services
Configure network firewalls to block unauthorized IP addresses.	Director of Network and Infrastructure Services
Install antivirus software.	Director of Network and Infrastructure Services
Employ a backup solution that automatically and continuously backs up critical data and system configurations.	Network and Infrastructure Specialist
Regularly test the restoration of data.	Network and Infrastructure Specialist
Disable port forwarding (disable the ability to connect over the internet with other public or private computers).	Network and Infrastructure Specialist
Sign up for Dorkbot web application vulnerability notification service.	Director of Network and Infrastructure Services
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 cyber incident and disseminate it to relevant parties.	Chief Information Officer

Mitigation Phase Reduce the impact of a cybersecurity incident.	
College Actions	**Responsible Role (Position responsible for this action)**
Conduct continuous scans on devices for additional vulnerabilities.	Network and Infrastructure Specialist
Provide updates on all 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 Support Specialist
Set antivirus and anti-malware solutions to automatically update and conduct regular scans.	Director of Network and Infrastructure Services
Separate student networks from other sensitive college networks where possible.	Director of Network and Infrastructure Services
Apply the Principle of Least Privilege (PoLP) to all systems and services so that users only have the access they need to perform their jobs.	Director of Network and Infrastructure Services
Require Multi-Factor Authentication (MFA) for accessing critical systems and consider using for all systems.	Director of Network and Infrastructure Services
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.	Director of Network and Infrastructure Services
Close or block network ports that are not in use to reduce the threat landscape of potential attacks.	Director of Network and Infrastructure Services

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

Response Phase

College 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.

This 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 college 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.

Section 5.0 - Documents

Document 1: Anomalies Report

Reporting System for Anomalies

It is essential to report computer anomalies, system performance issues, strange defects in operation, etc., to the Chief Information Security Officer. 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**
Date of Indication of Compromise		**Time of Indication of Compromise**	
Manufacturer		**Operating System (OS)**	
Description of Behavior			

Document 2: Services Restoration Priority Worksheet

This restoration worksheet identifies the services and systems used by the college to conduct its internal and external operations. Prioritizing services and systems is critical to supporting 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 college 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 college operations.
- *Tier 3:* Routine business functions and services that support college 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	Dell VxRAIL	Virtual Server Environment for all core services	All Users
	FortiVoice	Main Phone Communication with all employees	All Employees
	Astound or Charter Internet Services	Provides outside communication for college	All Users
	Power or Generator Services	Provides power to the datacenter	All Users
	FortiMail	Main email filter for college	All Users
	FortiSIEM/Analyzer	Provides security monitoring services to aid with incident response	Incident Response Team
2	Domain Controllers	Provides logon privileges inside the network	All Users
	Colleague servers	Core ERP system	All Users
	Colleague API servers	Provides external connections to ERP systems	All Users
3	Virtual Desktop Infrastructure	Provides remote computer resources	Some students
	Computer Labs	Computer resources across campus	Some students
	Print Servers	Print services	All users
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 college'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 and maintain devices and provides a starting point to prioritize disaster recovery efforts.

Temple College's Hardware and software inventory is managed by inventory software and will be attached as an appendix to this document.

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

College's actions during a cybersecurity incident.

College 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 College Network	**Chief Information Officer, Chief Information Security Officer**
When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.	**Chief Information Security Officer, Director of Network and Infrastructure Services**
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.	**Chief Information Security Officer, Director of Network and Infrastructure Services**
Block compromised systems from communicating with other devices or with attackers.	**Director of Network and Infrastructure Services**
Seek legal guidance ***before*** initiating communications.	**Chief Information Officer**
Contact a cyber insurance provider or broker if the college has an existing policy.	**Director of Purchasing**
Contact all critical software vendor(s).	**Chief Information Officer**
Contact the FBI, Law Enforcement, and Homeland Security, if needed.	**Chief Information Officer, Chief Information Security Officer**
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week by using the SB 271 Security Incident Reporting portal. If the college needs urgent support, they should call (877) 347-2476 (877-DIR-CISO). Colleges must report anomalous cyber activity and cyber incidents to DIR within 48 hours after discovery, and again within 10 days of incident closure.	**Chief Information Officer, Chief Information Security Officer**

During a Cybersecurity Incident

College's actions during a cybersecurity incident.

College Actions	Responsible Role (Position responsible for this action)
Consult with trained forensic investigators for advice and assistance ***prior*** to implementing any recovery or forensic efforts.	**Chief Information Officer, Chief Information Security Officer**
Contact banks, credit card companies, and other financial accounts to report that someone may be using the college's identity. Holds may need to be placed on accounts that have been attacked. Unauthorized credit or charge accounts will need to be closed.	**Director of Purchasing**
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.	**Chief Information Security Officer**
Oversee and track containment and restoration activities, including actions taken, resource assignments, and notifications.	**Chief Information Officer**
Track incident expenses.	**Chief Information Officer**
Initiate Continuity of Operations Plan (COOP) and essential department continuity plans.	**Chief Information Officer**

After a Cybersecurity Incident

Return to normal college operations following a cybersecurity incident.

College 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 Information Officer**
Conduct a root cause analysis to pinpoint where a malicious incident took place, then report to DIR within 10 business days.	**Chief Information Security Officer**
Communicate with internal and external stakeholders and manage public relations and reputation, including parents of students, if necessary.	**Executive Director of Communications**

After a Cybersecurity Incident

Return to normal college operations following a cybersecurity incident.

College Actions	Responsible Role (Position responsible for this action)
Conduct continuous monitoring of networks after a breach for any abnormal activity and make sure intruders have been inhibited thoroughly.	**Director of Networks and Infrastructure**
Work with affected system and service owners and managers to determine resources and sequencing needed to restore operations to a normal state.	**Director of Networks and Infrastructure**
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.	**Director of Networks and Infrastructure**
Track restoration efforts and provide information to the emergency management team (EMT) regarding estimated and actual time to full restoration.	**Chief Information Officer**
After ensuring evidence has been preserved for legal and insurance purposes, and given the all-clear, eliminate all traces of the incident.	**Chief Information Security Officer**
Activate the damage assessment team.	**Chief Information Officer**
Track damages and expenses for reimbursement claims.	**Chief Information Officer**
Conduct an After-Action Review (AAR) to identify areas of improvement for the incident response plan.	**Chief Information Officer, Chief Information Security Officer**
Develop and implement an Improvement Plan that includes recommended changes from the incident debriefing and AAR.	**Chief Information Officer, Chief Information Security Officer**
Share lessons learned through appropriate channels.	**Chief Information Officer, Chief Information Security Officer**
Contact DIR using the cybersecurity hotline which may be reached 24 hours, 7 days a week by using the **SB 271 Security Incident Reporting portal**. If the college needs urgent support, they should call (877) 347-2476 (877-DIR-CISO). Colleges must report anomalous cyber activity and cyber incidents to DIR within 10 days of incident closure.	**Chief Information Officer, Chief Information Security Officer**

After a Cybersecurity Incident Return to normal college operations following a cybersecurity incident.	
College Actions	**Responsible Role (Position responsible for this action)**
Colleges 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.	**Chief Information Officer, Chief Information Security Officer, Executive Director of Communications**

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
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.
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.

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

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.

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.

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.