Transforming How
Texas Government
Serves Texans

Incident Response Team Redbook

Texas Department of Information Resources
Office of the Chief Information Security Officer

February 2024

Table of Contents

Introduction

Need assistance with a cybersecurity incident? Call our 24/7 hotline at (877) DIR-CISO or (877) 347-2476

When a cybersecurity incident occurs, it is imperative that your organization has a plan in place for resolving the cybersecurity incident. This plan, called a Redbook or an incident response plan (and usually referred to internally as an IRP), includes comprehensive protocols and instructions for successful resolution of the incident. It instructs an incident response team (or IRT) on the steps to take before, during, and after a cybersecurity incident, and covers topics such as satisfying statutory reporting requirements, documenting actions taken, and establishing plans for responding to and resolving the incident.

The Texas Department of Information Resources (DIR) developed this Incident Response Redbook (hereafter referred to as "Redbook") with two guiding principles in mind:

- Every organization must pre-plan, develop, and maintain an incident response plan.
- Every organization must test and update the plan periodically to ensure its continued applicability.

Using This Document

DIR intends for this Redbook (along with corresponding template) to serve as a framework for an organization to use when developing its own incident response plan. It can and should be modified to meet your organization's business needs.

The Redbook includes instruction, information, templates, and references that you are encouraged to use to inform and structure your organization's incident response plan. It includes attachments that provide additional information covering a general incident response process.

When picking up the Redbook for the first time, you are encouraged to review the content and principles identified, consider what template sections would enhance your incident response plan, and become familiar with the attachments.

Reading the Redbook in its entirety can give you a comprehensive understanding of incident response and creating your own incident response plan. However, feel free to select and use sections of the Redbook that will result in the greatest benefit and value to your organization.

Part One - Getting Started

Developing an incident response plan from the ground up may seem daunting; however, many of the components of an incident response plan likely already exist within your organization. The resources in this Redbook can assist your organization by consolidating existing components and identifying any necessary new procedures to document and add structure to your organization's incident response process.

Part One – Getting Started provides an overview of the primary steps you should consider when developing an incident response plan. The primary steps for developing an incident response plan include:

Identify Your Incident Response Team Members

Deciding which personnel will comprise the incident response team is one of the first considerations to make when implementing an incident response plan. After finalizing who is going to be on the incident response team, you should identify what each person's roles and responsibilities will be, establishing a hierarchy for critical decision making and technical roles. Make sure to clearly document who will activate the incident response team, how the incident response team will activate, and how authority will be delegated to the response team coordinator. Your plan should contain a list of all incident response team members' after-hours contact information. Lastly, you should also consider how to update leadership about the incident, how to coordinate the response across multiple teams or departments, and how the incident response team will communicate during an incident.

Identify and Document External Support Resources

Establishing relationships with law enforcement and other support agencies before an incident occurs can be a great way to ensure that you have the correct contacts and resources in place before they are needed. You may consider joining organizations such as the Texas Information Sharing and Analysis Organization (TX-ISAO) or the Multi-State Information Sharing and Analysis Center (MS-ISAC). You can also use the Key External Contact Information Sheet template to capture external contacts that you may need during the incident response process. Regardless of which organizations you join, gather the necessary contact information and engagement requirements before you need them, so you can easily follow your incident response plan when the time for implementation comes. Because some external resources have associated costs, you should determine who in your organization will have the authority to activate these resources and what cost threshold that person is authorized to spend before requiring leadership approval or needing to comply with additional procurement and contracting requirements.

Develop Communication and Reporting Procedures

Coordinating with leadership during the planning process allows your organization to direct meaningful and actionable notifications to the correct audience, which reduces alert fatigue and avoids unnecessary notifications. You should define your organization's incident thresholds and identify who needs to be notified based on the initial incident analysis and triage findings. To be fully prepared for an incident, you may consider developing template press releases and sample internal and external cybersecurity incident notifications. You are encouraged to reference and customize the Redbook's templates for initial incident reporting and ongoing situational reporting to keep your organization's leadership informed on the status of an incident or the incident response team.

Classify Data, Document Systems, and Develop a Network Diagram

Determining the classification of your organization's data and documenting where and how your organization maintains its systems, networks, and endpoints can help inform your incident response team's decision-making processes when an incident occurs. Understanding if your organization maintains information that is regulated, confidential, sensitive, or public will inform potential legal and reputational risks during incident response. You should consider classifying your data and developing system diagrams to ensure that you know what your systems contain, how your systems interact, what type of data could have been compromised, and what can be taken offline during an incident. Accurate systems and data documentation may also aid in system recovery and risk assessments when resolving the impact of a cybersecurity incident. Make sure to identify the business units responsible for maintaining these asset inventories and keep both digital and hard copies of these documents.

Understand Relevant Incident Reporting Requirements

Your organization may be required to report cybersecurity incidents to state officials, federal officials, or industry representatives based on the severity and scope of the incident and the data impacted. As part of your incident response planning process, identify possible statutory and contractual obligations for reporting incidents to federal officials, state officials, insurance vendors, risk pool providers, and other organizations.

Define Action Items for Each Phase of the Incident Response Plan

By pre-planning incident response activities, your organization can execute the critical steps necessary to contain a cybersecurity incident and set expectations for the remediation and recovery of impacted systems. You should comprehensively define, carefully consider, and thoroughly document the key action items of your incident response plan for each phase of the incident response life cycle. Anticipate what, if any, additional technical expertise will be needed to support a potential forensic investigation. Coordinating with your organization's leadership to prioritize any necessary additional technical expertise, such as evidence collection and forensic analysis, will allow the response team to determine the root cause of the incident and build resilience during the recovery phase.

Continuously Improve

Continuous and consistent evaluation of the incident response plan ensures that it stays accurate, up to date, and top of mind. You should evaluate and improve the incident response process based on feedback from previous incidents and exercises, incorporating lessons learned into the incident response plan and making improvements to your processes based on the after-action review and corrective action plan.

Build a Culture of Cybersecurity Within Your Organization

While there is no single way to build a cybersecurity program, establishing an organizational culture of safety, honesty, and transparency can lay the groundwork for the successful activation of the incident response plan. A culture of cybersecurity should come from leadership and encourage thoroughness, availability, and consistency.

Part Two – Background, Guidance, and Reference

Part Two – Background, Guidance, and Reference provides background information and technical guidance, and acts as a reference for best practices as organizations build out their incident response plans or programs.

Incident Response Planning Goals

The Cybersecurity and Infrastructure Security Agency (CISA) defines an incident response plan as a written document formally approved by the senior leadership team, which helps your organization before, during, and after a confirmed or suspected cybersecurity incident.[1] The incident response plan will clarify roles and responsibilities and provide guidance on key action items.

The incident response plan will clarify roles and responsibilities and provide guidance on key action items.

An incident response plan may include the following sections:

- Objectives and goals of the incident response plan.
- Organizational structure of the incident response team.
- Incident response training and exercise expectations.
- Roles and responsibilities of the response team members.
- Contact information for internal team members and external resources.
- Incident response activities identified by phase.
- Incident triage and communication thresholds.
- Considerations for system recovery and post-incident activities.
- Considerations for incident communication.

The resources in this Redbook will help inform organizations as they mature their own incident response programs and formalize their incident response plans.

Security Incident Triage Checklist

The following steps support an investigation into the cause, scope, and potential complexity of a cybersecurity incident in addition to guiding the mitigation and containment of future impacts and associated risks.

An organization should consider the below steps and potential actions when responding to a potential cybersecurity incident:

[1] CISA Incident Response Plan (IRP) Basics

1. **Assemble the incident response team**: Assemble the team in response to the incident.
2. **Secure data and information systems**: Secure data and confidential information to limit immediate consequences of the incident. Isolate servers and systems to mitigate the incident.
3. **Evaluate data elements and source**: Determine the type, owner, and amount of confidential information that may have been compromised. Identify each location where confidential information may have been compromised and who the business owner of the confidential information is.
4. **Identify scope and escalation**: Confirm the degree of impact to the data or systems.
5. **Notify management**: Advise appropriate internal management of the incident.
6. **Determine the number of individuals impacted**: Determine the number of individuals impacted. Notify applicable parties if the incident meets breach notification requirements, either individually or through a media announcement, based on applicable laws.
7. **Determine discovery date**: Determine the date the agency or contractor knew—or should have known about—the incident.
8. **Execute external communications as required**: Advise external contacts as required, such as DIR, legislative leadership, the Office of the Attorney General, Secretary of State (SOS), law enforcement, or any other applicable regulatory authority. If a breach resulted in the unauthorized release of sensitive personal information, notify the individuals impacted as required by the Identify Theft Enforcement and Protection Act[2] or other applicable law.
9. **Investigate**: Interview, analyze, and document all current findings regarding the incident.
10. **Mitigate**: Revise policies, process documents, or business requirements and enforce contracts to reduce the likelihood of incident reoccurrence.

Incident Impact Analysis

An organization should conduct an incident impact analysis during an incident investigation to accurately categorize the incident's impact on the organization's business functions. Accurately categorizing an incident's impact level determines what steps to execute in your incident response plan. Once you determine the incident's initial impact level, you may need to escalate the incident notification or contact additional resources for support.

Accurately categorizing an incident's impact level determines what steps to execute in your incident response plan.

The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (Special Publication NIST 800-61) provides recommendations on prioritizing the severity of

[2] Gov't Code Chapter 521.

cybersecurity incidents. Section 3.2.6 Incident Prioritization identifies the following factors for incident impact level classification:

- **Functional Impact**: Incidents targeting IT systems typically impact the business functionality provided by those systems, resulting in a negative impact to system users.
- **Information Impact**: Incidents may affect the confidentiality, integrity, and/or 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 recovery.[3]

While there is no single model for determining incident impact level, you should strongly consider a model that identifies the thresholds, terms, and recoverability categories described in the succeeding sections, which each provide guidance on defining an incident's impact on an organization. These examples consider impacts to systems, infrastructure, and an organization's ability to recover from an incident. Organizations should consider each category to assure proper response and recovery from an incident.

You should strongly consider an incident impact level model that identifies thresholds, terms, and recoverability categories.

Functional Impact Thresholds

The thresholds below are based on CISA's National Cyber Incident Scoring System (NCISS). The NCISS priority levels have been adjusted to reflect the state level thresholds.

- **Emergency**: An incident meets the emergency threshold if it impacts critical infrastructure systems or curtails delivery of public health and medical services, power generation and distribution services, water and wastewater utilities, telecommunications systems, government operations, or public safety services.
- **High**: An incident meets the high threshold if it results in noticeable impact to government operations, infrastructure systems, or public safety systems, or if it reduces public confidence in an entity's service delivery.
- **Medium**: An incident meets the medium threshold if it results in the degradation of an organization's programs or services, or if it reduces public-facing service delivery capacity.
- **Low**: An incident meets the low threshold if it impacts individual users or accounts.

Impact Terms

Organizations should define terms and definitions that will be used in their incident response plans to avoid confusion when discussing cybersecurity incidents. Examples include:

- **Event**: Any observable occurrence in a network or information system.[4]

[3] NIST Computer Security Incident Handling Guide (Special Publication 800-61, Revision 2)

[4] NIST Risk Management Framework for Information Systems and Organizations (Special Publication 800-

- **Incident**: A security event that compromises the integrity, confidentiality, or availability of an information asset.
- **Breach**: An incident that results in the confirmed disclosure of data to an unauthorized party.[5]

Recoverability Effort Categories

Because recovery efforts will look different when responding to a cybersecurity incident, organizations should define recoverability effort categories that make sense for their industry and business needs, such as:

- **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 (for example, sensitive data has been exfiltrated or leaked and then posted publicly); the incident requires a significant investigation.

Escalation Criteria

NIST's Computer Security Incident Handling Guide provides recommendations on how and when to escalate a cybersecurity incident.

Incident Escalation: Communication

Section 3.2.7 Incident Notification outlines important contacts and modes of communications for resolving cybersecurity incidents.

Example key contacts include:

- Chief elected official.
- Chief executive officer.
- Chief information officer.
- Chief privacy officer.
- Head of information security.
- Local information security officer.
- External incident response resources.
- System owner.
- Human resources.
- Public affairs or media and communications.
- Legal department.

Your organization should establish an escalation process containing associated notification thresholds to ensure the appropriate members in your incident response plan are notified of a potential or actual cybersecurity incident. Not every contact in your incident response plan will be notified for each

Not every contact in your incident response plan will be notified for each cybersecurity incident.

37, Revision 2)

[5] Verizon 2021 Data Breach Investigations Report

cybersecurity incident your organization experiences. For example, for low threshold incidents, your incident response plan might only tap the system owner and local information security officer for resolution of the incident.

In Part Three, page 12 of this document the Incident Response Team Templates provides additional sample internal and external contacts templates for structuring your organization's incident notification process.

Breach and Security Incident Notification Requirements

Some cybersecurity incidents may result in the disclosure of private, confidential, or regulated data. The following sections include breach and incident notification requirements in the state of Texas. This information is provided for informational purposes only. These sections are not intended to serve as legal advice nor are they an exhaustive list of all legal requirements. You should consult your organization's legal counsel for more detailed information.

Texas Identity Theft Enforcement and Protection Act

State agencies, local governments, and organizations conducting business in the state must report certain security breach incidents pursuant to the Texas Identity Theft Enforcement and Protection Act.

An organization must disclose to an impacted individual that an incident has exposed their sensitive personal information (SPI). An organization must also disclose to the Office of the Attorney General an incident that exposes the SPI of 250 or more individuals.

For additional details, reference the following:

Statute	Summary
Business & Commerce Code Section 521.053	Explains when business owners must notify an individual that a breach exposed their SPI.
Government Code Section 2054.603	Explains when state agencies and local governments must notify an individual that a breach exposed their SPI and when these entities must notify DIR of a security incident.
Local Government Code Section 205.010	Explains when local governments must notify an individual that a breach exposed their SPI.

Resources

- Report a Data Security Breach

Local Government Cybersecurity

Effective September 1, 2023, local governments must report security incidents[6] to DIR.

To report a local government cybersecurity incident:

1. Navigate to the Cybersecurity Incident Management and Reporting webpage.
2. Click **Access Archer Engage**.

[6] Gov't Code § 2054.603(a)(1); *see also* 1 Tex. Admin. Code § 202.1(41).

3. Sign in to Archer Engage. (**Sign up** first if you do not have access to Archer Engage.)
4. Follow the prompts and submit the report when complete.

For additional details, reference the following:

Reference	Summary
Government Code Section 2054.603	Explains when local government entities must notify DIR of a security incident.
Texas Administrative Code Section 202.23 (e)	Defines the type of security incidents local governments must report to DIR.

Resources

- Local Government Incident Reporting User Guide

School Cybersecurity

Independent school districts and open-enrollment charter schools must report cybersecurity incidents that constitute a breach of system security to the Texas Education Agency (TEA) or other appropriate entity as soon as practicable after the discovery of the cyberattack or cybersecurity incident.

To report a school cybersecurity incident:

1. Navigate to the Cybersecurity Incident Management and Reporting webpage.
2. Click **Access Archer Engage**.
3. Sign in to Archer Engage. (**Sign up** first if you do not have access to Archer Engage.)
4. Follow the prompts and submit the report when complete.

For additional details, reference the following:

Statute	Summary
Education Code Section 11.175	Explains when independent school districts and open-enrollment charter schools must notify the appropriate state agencies and an individual's parents that a breach has exposed SPI.

Resources

- Local Government Incident Reporting Web Form Submission Guide

Election Cybersecurity

If the county election officer becomes aware of a cybersecurity incident that impacts election data, the officer must immediately notify the Texas Secretary of State.

For additional details, reference the following:

Statute	Summary
Election Code Section 279.003	Explains when county election officers must notify the Texas Secretary of State that a breach has exposed information that is

Statute	Summary
	created or managed in the operation of an election system.

State Level Security Incident Reporting

State agencies and institutions of higher education are directed by Government Code Section 2054.603(b)(3) to comply with DIR's security reporting rules.[7] DIR's rules require an entity to report a security incident to DIR within 48 hours of discovery where the incident is assessed to have:

- Propagated to other state systems;
- Resulted in criminal violations (that shall be reported to law enforcement in accordance with information cybersecurity and privacy laws);
- Involved the unauthorized disclosure or modification of confidential information, including SPI; or
- Been an unauthorized incident that compromises, destroys, or alters information systems, applications, or access to such systems or applications in any way.

To report an urgent incident:

1. Navigate to the Cybersecurity Incident Management and Reporting webpage.
2. Click **Access SPECTRIM**.
3. Login to SPECTRIM.
4. In the Incident Mgmt tab, click **Report New Incident** and enter the appropriate incident details.

For additional information, reference the following:

Statute/Rule	Summary
Government Code Section 2054.603	Explains when state agencies and local governments must notify DIR of a breach or suspected breach.
Texas Administrative Code Section 202.23 (d)	Explains when state agencies and local governments must notify DIR of a security incidents.
Texas Administrative Code Section 202.73 (d)	Explains when institutions of higher education must notify DIR of security incidents.

Resources

- Report an Urgent Incident via SPECTRIM

[7] 1 Tex. Admin. Code §§ 202.23, 202.73.

Data Classification Definitions and Guidance

The DIR Data Classification Guide outlines four proposed labels that can be applied to your organization's data. When developing a data classification policy, organizations should consider the following four data categories.

- **Public**: Information that is freely—and without reservation—made available to the public.
- **Sensitive**: Information that could be subject to release under an open records request, but should be controlled to protect third parties
- **Confidential**: Information that typically is exempted from the Public Information Act.
- **Regulated**: Information that is controlled by a state or federal regulation or other third-party agreement.

Post-Incident Analysis and Activity

The Computer Security Incident Handling Guide (NIST 800-61) outlines potential incident analysis activities an incident response team should perform after an incident.

Section 3.4 of the Guide, titled "Post Incident Activity," outlines guidance for capturing lessons learned and analyzing post-incident and root cause issues using collected incident data.

Learning and Improving

To improve cybersecurity measures and incident handling processes, an incident response team should conduct an after-action review with all involved parties after a major incident (and periodically after lesser incidents as resources permit).

A cybersecurity review after an incident should address:

- What happened and at what times during the incident?
- Were documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What might staff and management do differently should a similar incident occur?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Follow-Up Reporting

Creating an after-action report (AAR) for an incident provides a structured analysis that you can use to assess and improve your incident response team's response times, executed actions, and more.

After-action reports typically include:

- A formal incident chronology (including time-stamped information from systems).

- A monetary estimate of the amount of damage the incident caused.
- Follow-up reports as specified by an organization's retention policies.

Data Collected

Organizations should collect and retain data and information that is relevant to the incident.

Data collected may include:

- Forensic images and logs.
- Situational reports.
- Incident handling notes.
- Decision documents.
- Incident cost-tracking documents.
- Personal time-tracking documents.

Root Cause Analysis

Organizations performing root cause analysis should focus on relevant objective assessment activities.

Root cause analysis typically includes:

- Reviewing logs, forms, reports, and other incident documentation.
- Identifying recorded precursors and indicators of compromise.
- Determining if the incident caused damage before it was detected.
- Determining if the incident was a recurrence of a previous incident.
- Calculating the estimated financial or reputational impact of the incident.
- Determining the accuracy of the initial impact assessment.
- Identifying what could have prevented or mitigated the impact of the incident.

Part Three - Incident Response Team Templates

Part Three – Incident Response Team Templates provides templates relevant to the development and operation of an incident response team. These templates detail guidelines that an organization may incorporate into their own incident response plan. You may alter the templates as necessary for your needs. Your incident response team should maintain both hard and digital copies of the incident response plan.

Your incident response team should maintain both hard and digital copies of the incident response plan.

The plan sponsor or owner should be responsible for modifying these templates for the incident response team's use. Brackets, both those [without shading] and those [with blue shading], indicate where the templates should be customized to reflect your organization's needs; however, you are encouraged to modify all sections of the template as necessary, not just those that DIR intends to be customized.

TLP: AMBER

Limited disclosure, restricted to participants' organization and its clients.

The information in this document may be confidential
pursuant to Texas Government Code § 552.139.

[Organization Name]

Information Cybersecurity Incident Response Team Redbook

Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any third-party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.

Role	Name	Phone	Email
Sponsor*	[Sponsor name]	[Sponsor phone]	[Sponsor email]
Owner**	[Owner name]	[Owner phone]	[Owner email]
*Sponsor is the executive responsible for compliance **Owner is the owner of this document			
Last Document Update: [mm/dd/yyyy]			

Incident Response Team Overview

Purpose

This Incident Response Plan establishes membership, roles, responsibilities, and activities of the [organization name] response team in preparation for an actual or suspected cybersecurity incident.

Incident Response Team Mission

The response team's mission is to support incident response preparedness and build a program that can identify and detect actual or suspected cybersecurity incidents. The response team also responds to and contains, eradicates, and supports the recovery of cybersecurity incidents.

Scope

This plan applies to any computing devices owned or leased by the organization, personal devices used to access the organization's cloud resources, and cloud-hosted systems as appropriate. Incident response roles and responsibilities are documented in the organization's response plan.

[Organization name] established a response team to respond to cybersecurity incidents. The response team operates on behalf of the [organization name]'s leadership and engages, informs, and receives support from the Response Team Coordinator. It is comprised of personnel with expertise in responding to a significant actual or suspected cybersecurity incident who are involved in decision making and prioritizing incident response activities. Members of the Leadership Team will designate appropriate personnel for the response team.

There [is/is not] a set protocol to initiate the response team activities in response to an actual or suspected incident. Once activated, the response team is authorized to [require compliance with the organization's established procedures/request cooperation/establish incident response priorities that may supersede daily operational responsibilities/require attention outside normal business hours].

Incident Response Team Leadership and Responsibilities

The Response Team Coordinator (hereafter referred to as the Coordinator) is designated by and reports to [Leadership Position]. The Coordinator manages all aspects of the response, coordinates direct communication, and ensures necessary notifications are made to the appropriate individual or organization. The Coordinator is the primary internal point of contact during the response.

The incident response team may conduct the following activities, aligned to the incident response life cycle:

- **Preparation**: Plan for incident response, train on incident response roles, and conduct exercises of incident response plans and procedures.
- **Detection and Analysis**: Support detection of cyber threats and define the methods used to analyze the potential impact of an incident.
- **Containment, Eradication, and Recovery**: Quickly respond to limit the impacts of an incident, remove any threat actor persistence in the organization's systems, and support

the recovery of the organization's systems to pre-incident conditions.

- **Post-Incident Recovery**: Conduct an after-action review and develop a corrective action plan to continually improve the organization's response to incidents.

Example incidents that may fall within the response team's responsibility include, but are not limited to:

- Malware infection, including a computer virus, worm, bot, crypto miner, or trojan.
- Sustained denial of service (DDoS) attack.
- Ransomware infection impacting computers or servers.
- Disclosure of non-public or sensitive data.
- Incidents that are likely to be high-profile or create a significant risk of financial, reputational, or physical harm.

A member of the leadership team may determine whether a scenario that is not described or considered by this Redbook constitutes a significant incident.

Incident Response Team Structure

[The table below provides options for structuring your organization's incident response team.]

Team	Function	Members
Leadership Team	The Leadership Team has decision-making authority to guide incident response priorities and activities, and provides command objectives and institutional knowledge. The Leadership Team prioritizes the work of the Core Team and addresses the organizational or managerial components of incident response.	• Chief Elected Official • Chief Executive Officer • Executive Management • IT/Technology Directors • Incident Response Team Coordinator • Legal • Communications • Other positions as needed
Core Team	The Core Team facilitates activities to detect, respond to, contain, eradicate, and recover from a cybersecurity incident. The Core Team works the Extended Response Team to aid with incident resolution and may serve as subject matter experts on privacy, cybersecurity, or technical Information Technology (IT) systems.	• IT Infrastructure • IT Applications • Third-Party Security Vendors • Other positions as needed
Extended Response Team	The Extended Response Team provides unique subject matter expertise in their respective fields and may support incident response activities.	• Human Resources • Facilities • Law Enforcement

Team	Function	Members
	The Extended Response Team may serve as subject matter experts on matters relating to their specific business or operational function.	- Emergency Management - Other positions as needed

Incident Response Team Member Roles

[The table below identifies different positions on the incident response team. Customize the positions, their assigned team component, and roles based on your organization's operational needs, capability, and structure.

The positions and responsibilities described below are based upon best practices in the information privacy and cybersecurity industries. This does not indicate that the example responsibilities are appropriate or necessary for your organization.]

Team Member Roles

Position	Team	Responsibilities
Incident Response Team Coordinator	Leadership Team	- Serves as the primary point-of-contact for incident response activities. - Coordinates incident triage and declaration. - Establishes, maintains, and updates written response team protocols or incident response plans. - Identifies roles and responsibilities for response team members. - [Add additional duties based on organizational requirements]
Chief Elected Official Executive Officer or Executive Director	Leadership Team	- Holds ultimate accountability for preparedness, response, and recovery activities. - Monitors the impact to services and recovery efforts. - Communicates with counsel, court, or commission members. - [Add additional duties based on organizational requirements]
City Manager, County Administrator, Superintendent, or Deputy Director	Leadership Team	- Monitors incident response activities and maintains situational awareness of incident response functions. - Coordinates with external affairs and communication staff on public notices.

Position	Team	Responsibilities
		• Manages information flow between impacted business units. • [Add additional duties based on organizational requirements]
IT/Technology Director or Information Security Officer	Leadership Team	• Monitors incident response activities and maintains situational awareness of incident response functions. • Updates leadership, and coordinates management-level decisions and actions. • [Add additional duties based on organizational requirements]
Legal Counsel	Leadership Team	• Advises on legal compliance matters, such as breach notification laws and privacy compliance. • [Add additional duties based on organizational requirements]
Privacy Officer	Leadership Team	• Coordinates and monitors breach notification activities. • [Add additional duties based on organizational requirements]
Communications/External Affairs	Leadership Team	• Manages all public communications regarding incidents and may rely on input from technical subject matter experts to craft public messages. • [Add additional duties based on organizational requirements]
IT Infrastructure or Applications Manager	Core Team	• Supports incident response activities in alignment with the incident response life cycle and industry best practices. • Provides situational updates to the response team coordinator. • [Add additional duties based on organizational requirements]
System/Network Administrators	Core Team	• Supports incident response activities in alignment with the incident response life cycle and industry best practices. • Provides situational updates to the response team coordinator. • [Add additional duties based on organizational requirements]

Position	Team	Responsibilities
Forensic or Cybersecurity Technicians/Consultants	Core Team	• Supports incident response activities in alignment with the incident response life cycle and industry best practices. • Provides situational updates to the Incident Response Team Coordinator. • [Add additional duties based on organizational requirements]
Human Resources	Extended Response Team	• Manages internal communications to employees regarding incident status and may coordinate with technical subject matter experts to craft communications. • Monitors response team activity and supports staff time tracking. • [Add additional duties based on organizational requirements]
Law Enforcement	Extended Response Team	• Supports incident investigation and maintains chain of custody of forensic evidence. • Provides physical security for response team. • Coordinates with appropriate law enforcement partners. • [Add additional duties based on organizational requirements]
Emergency Management	Extended Response Team	• Provides logistical support for response team activities. • Coordinates with leadership team to support the organization’s continuity of operations. • Coordinates with regional and state level emergency management partners for resource support and situational awareness. • [Add additional duties based on organizational requirements]
Finance/Purchasing	Extended Response Team	• Provides purchasing and contract support for incident response activities. • Tracks expenses incurred by the incident response team. • [Add additional duties based on organizational requirements]

Position	Team	Responsibilities
Facilities	Extended Response Team	• Provides access to facilities and building locations to response team members. • Supports the activities of the response team as needed. • [Add additional duties based on organizational requirements]

Incident Response Team Member Contact Information

[The following table contains contact information for the organization’s incident response team members.]

Response Team Contact Information

Position	Name	Phone	Email	After-Hours Contact
[Sample Position Name]	[Jane Smith]	[512-555-5555]	[Jane.Smith @email.com]	[512-555-5555]
Response Team Coordinator				
Chief Elected Official				
City Manager				
County Administrator				
Superintendent				
IT Director				
Information Security Officer				
Legal Counsel				
Privacy Officer				
Communications/ External Affairs				
IT Infrastructure/ Applications Manager				
System/Network Administrator				
Forensic/ Cybersecurity				

Position	Name	Phone	Email	After-Hours Contact
Technicians/ Consultants				
Human Resources				
Law Enforcement				
Emergency Management				
Finance/Purchasing				
Facilities				
[Additional positions as needed]				

Key External Contact Information Sheet

[Based on legislative or regulatory mandates, organizations may be required to report cybersecurity incidents to specific individuals or government entities. This list provides contact information to support those notifications.]

External Contact Information

Entity or Organization	Title, Dept., or Location	Name	Phone	Email
Texas State Representative				
Texas State Senator				
[Chief Elected Official]				
[Manager or Administrator]				
Cyber Insurance Provider				
[Organization]				
[Organization]				
Texas CISO Office	DIR – Incident Response	DIR CIRT	1-877-347-2476 (24/7 hotline)	CIRT@dir.texas.gov

Entity or Organization	Title, Dept., or Location	Name	Phone	Email
Texas Division of Emergency Management	Assistant Chief			
	District Chief			
	State Operations Center (SOC)	Daily Ops	512-424-2208	soc@tdem.texas.gov
Texas DPS and Criminal Justice Information System (CJIS)	Regional Office			
	CJIS	DPS OIC	1-800-638-5387	securitycommittee@dps.texas.gov
	Texas Fusion Center	Real-Time Watch Center	512-424-7981	txfc@dps.texas.gov

High-Level Incident Response Process Overview

[The high-level process outlined in this document is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide.]

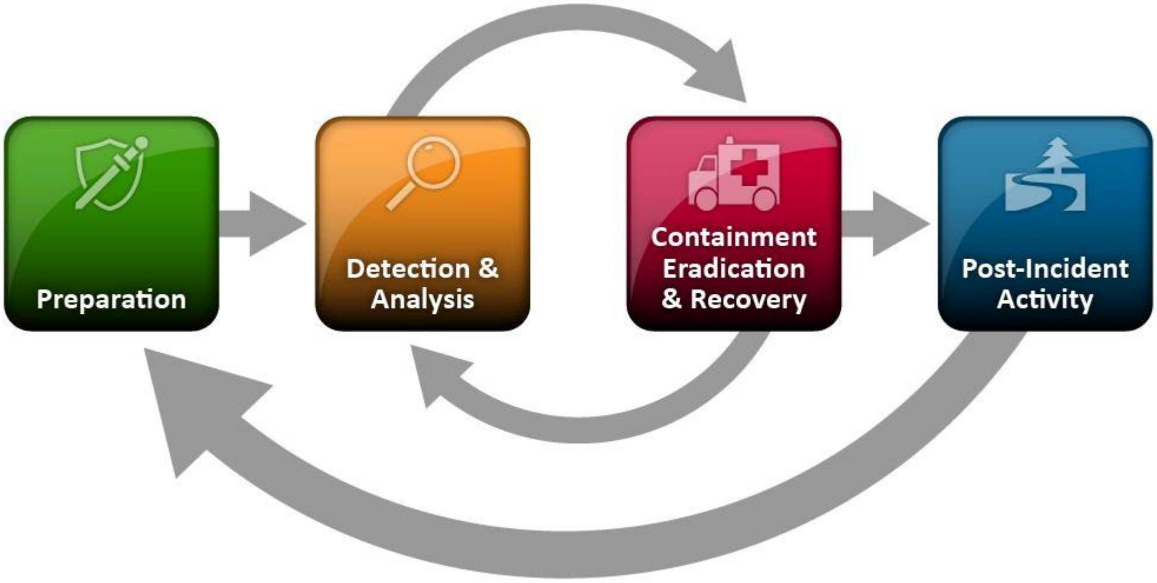

Figure .1 NIST Incident Response Life Cycle[8]

[The table below outlines key activities and considerations during the incident response life cycle.]

[8] NIST Risk Management Framework for Information Systems and Organizations

Incident Response Phase and Description/Activities

Phase	Description/Activities
Preparation	**Preparation** activities include activities performed in advance of a cybersecurity incident that help increase the resilience of an organization, reduce the impact of a cybersecurity incident, or improve the organization's ability to effectively respond to and recover from an incident. Some common preparation activities include: • Establishing an incident response team. • Developing and testing an incident response plan and procedures. • Increasing the resilience of systems, networks, and backups. • Conducting user awareness and training activities. • Managing vulnerabilities and securing networks and systems. • [Add additional containment steps based on organizational requirements] Additional preparation best practices may be found on page 3 of the MS-ISAC/CISA Joint Ransomware Guide.
Detection and Analysis	**Detection and analysis** activities determine when an observed anomaly or event is a true information privacy or cybersecurity incident. A true incident should be classified and prioritized to determine the appropriate response. Some common detection and analysis activities include: • Analyzing precursors for signs of a potential attack, which may include targeted threat intelligence, known vulnerabilities being exploited, or network scanning and enumeration. • Analyzing indicators to determine their potential impact, which may include network intrusion alerts, anti-virus or enhanced detection and response (EDR) warnings, unauthorized system changes, or pre-staged files in sensitive locations. • Reviewing logs to coordinate potentially malicious events. • Identifying and triaging an incident to determine its type and scope of impact. • [Add additional containment steps based on organizational requirements] Each incident should be prioritized to ensure the appropriate resources are allocated to the response efforts. Additional detection and analysis activities can be found on page 11 of the MS-ISAC/CISA Joint Ransomware Guide.
Containment, Eradication, and Recovery	**Containment** of an identified incident limits further damage and reduces the business impact to the organization. Some common containment strategies include:

Phase	Description/Activities
	• Isolating the system. (Keep systems powered on to preserve volatile memory unless shutdown is required.) • Disabling services, protocols, or appliances. • Disabling account access. • [Add additional containment steps based on organizational requirements] Each incident may require unique containment strategies. Preserving evidence and collecting forensic images and logs during the containment phase may better enable threat eradication. Additional containment best practices can be found on page 12 of the MS-ISAC/CISA Joint Ransomware Guide. After an incident has been contained, **eradication** may be necessary to eliminate established threat actor persistence or to remediate an exploited vulnerability. Some common eradication strategies include: • Remediating or mitigating exploited vulnerabilities. • Removing malware or other malicious files. • Securing and resetting compromised user accounts. • [Add additional eradication steps based on organization requirements] Additional eradication best practices can be found on page 12 of the MS-ISAC/CISA Joint Ransomware Guide. In the **recovery** stage, any production systems affected by a threat will be rebuilt or reconstituted and brought back online, including data recovered from backups that has been determined to be safe from tampering. Some common recovery strategies include: • Rebuilding and reimaging impacted workstations and servers. • Sanitizing user and service accounts. • Segmenting network and reviewing back up strategy. • [Add additional recovery steps based on organization requirements] Additional recovery best practices can be found on page 14 of the MS-ISAC/CISA Joint Ransomware Guide.
Post-Incident Activity	**Post-incident activities** include: • Conducting a hot wash and after-action review to gather lessons learned from the incident (involve all parties that participated in incident response and recovery activities). • Recognizing gaps, reviewing policies and incident response plans, and identifying corrective actions to address gaps. • Considering opportunities to improve processes, coverage, and refine alerting of security tools.

Phase	Description/Activities
	- Conducting additional training for security and non-security staff. - Reviewing industry standards to ensure evidence retention requirements are met. - [Add additional recovery steps based on organization requirements] Additional post-incident best practices can be found on page 14 of the MS-ISAC/CISA Joint Ransomware Guide and in Post-Incident After-Action Review and Improvement Plan of this document.

Incident Analysis and Escalation

Determining the scope and severity of a cybersecurity incident is a critical step in allocating the appropriate resources to quickly contain and eradicate an emerging cyber threat. With the knowledge of the incident's complexity and scope, response team leadership can communicate business impacts to the appropriate internal and external stakeholders.

Incident Analysis

Once classified, current best practices recommend triaging the incident and assigning a severity level. Classification and triaging inform and direct incident escalation, while communicating the actual or potential impact to the organization. However, cybersecurity incidents are dynamic, and the severity level may change during an investigation or over the course of the response as more information is gathered and the investigation unfolds. Response team leadership is ultimately responsible for incident classification.

Incident Triage

The thresholds below are based on the Cybersecurity and Infrastructure Security Agency (CISA) National Cyber Incident Scoring System (NCISS). Incidents may be categorized based on the threshold of impacts identified in the sample table below.

[The provided template is one example of an incident triage framework for assessing the impact of a cybersecurity incident. Customize the Incident Triage template to fit the needs of your organization.]

Threshold	Impact Scope	Customer Impact	Continuity of Operations	Cost	Recoverability	Reputation
4 Emergency	Internal or external organization	Life safety systems impacted	Government services unavailable	>$$	Data lost and not recoverable	Significant risk for reputational harm
3 High	Entire organization	Customer-facing services inoperable	Department services unavailable	$ to $$	Data lost but manually recoverable	Potential for reputational harm due to service outages

Threshold	Impact Scope	Customer Impact	Continuity of Operations	Cost	Recoverability	Reputation
2 **Medium**	Multiple roles	Customer-facing services degraded	Single application unavailable	<$	Data lost but digitally recoverable	Limited potential for reputational harm
1 **Low**	Single role	No customer impact	No interruption	No cost	No data lost	No reputational impact

Observed functional impacts may not all align with the table above. Use best judgment when triaging an incident and adjust as more information becomes available.

Notification Thresholds

The appropriate staff and teams should be notified based on the severity of an incident. Observation of the communication thresholds is critical to reducing alert fatigue. The escalation threshold template provided below identifies required and recommended notifications based on the incident severity. In rapidly evolving situations, the severity may increase quickly, and additional individuals may need to be notified and back briefed.

[Customize the Notification Escalation Thresholds table to fit the needs of your organization. For example, if your organization has an Executive Director instead of an Organization Head or Chief Official, feel free to replace the positions in the table.]

Threshold	Notification Recommended	Notification Considered
4 **Emergency**	• [Name of position being notified] • Organization Head or Chief Official • Council or Commissioners Court • All positions at the High and lower threshold	• [Name of position being notified]
3 **High**	• [Name of position being notified] • Legal Counsel • Human Resources • Public Information Officer • All positions at the Medium and lower threshold	• [Name of position being notified] • Emergency Management • Law Enforcement
2 **Medium**	• [Name of position being notified] • Incident Coordinator • Incident Response Core Team • IT Director • All positions at the Low threshold	• [Name of position being notified] • Deputy Director
1 **Low**	• [Name of position being notified] • Help Desk • IT Manager	• [Name of position being notified]

Situation Notifications

In addition to the escalation thresholds, some situations require immediate notification to specific positions. These situations and points of contact are listed below.

[Customize the Notification Situations table to fit the needs of your organization.]

Situation	Point of Contact Notified
[Situation]	• [Name of position being notified]
Breach of Customer or Employee Information	• Privacy Officer • Legal Counsel • Public Information Officer
Critical Business Process Offline	• Business Unit Leader(s) • Organization Head
Ransom Demand	• Organization Head • Chief Elected Official • Legal

Services Restoration Priority Worksheet

The services restoration policy below identifies the services and systems used by the organization to conduct its internal and external operations. Prioritization of the importance or criticality of services and systems is paramount to supporting restoration priorities during incident response and recovery activities. These services and systems may be listed and prioritized as part of the business continuity or disaster recovery planning process.

[Consider the restoration priority for your organization using the sample classifications below:

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

Services Restoration Policy

[The table below provides a consolidated list to guide service restoration.]

Priority	Service/System	Function and Details	End User
1	[Domain controllers]	[Authentication – Active Directory]	[Internal and External]
2			

Priority	Service/System	Function and Details	End User
3			
4			

Hardware and Software Inventory

[Your organization should track its IT resources, including computers, servers, mobile devices, IP phones, internet connected devices, and approved and managed software. This inventory allows IT or the organization's managed service provider to track devices to maintain and provide a starting point for prioritizing disaster recovery efforts.]

Hardware Tracking

[You should consider using a hardware tracking spreadsheet that inventories your organization's current hardware.

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

Typically, a hardware tracking spreadsheet will capture a combination of the following:

- Asset Number.
- Current Status.
- Assigned Employee.
- Asset Type.
- Model.
- Manufacturer.
- Location.
- Description.
- Date Issued.
- Date Returned.]

Asset Number	Assigned Employee	Asset Type	Model	Manufacturer	Serial Number
[XXXXX]	[Jane Doe]	[Laptop]	[Model	[Dell]	[XXXXX]

Software Tracking

[Complete and maintain the following software tracking sheet. Customize the table, including headers, as appropriate. The Center for Internet Security (CIS) provides additional an hardware and software asset tracking spreadsheet if needed.]

Software Use	Name	Software Description	License Type	Version	Software Key	Purchase Date	Billing Cycle
[End User]	[Adobe Lightroom]	[Photo Editor]	[Service]	[X.X]	[In Console]	[MM/DD/YYYY]	[Monthly]

Data Classification Process

[Your organization should classify its data according to a defined schema. The process of data classification provides your organization insight into the risks associated with data breaches in addition to informing the implementation of appropriate security controls before an incident occurs.

DIR has developed a Data Classification Template for state agencies to use as a guide. All organizations may leverage this template to support the data classification process.

The table below identifies the responsibilities of sample data professionals who may work with data at your organization. These roles likely have different responsibilities, dependent upon data classification. These roles may be different than traditional incident response roles since these activities are largely conducted before an incident occurs.

This table can modified to suit your organization's needs.]

Role	Public	Sensitive	Confidential	Regulated
Data Custodian	• Ensure systems support access controls which enforce data classification.			
Data Owner	• Identify the classification level of data. • Review audit logs.			
Information Security Officer, Legal and/or Privacy Office	• Develop and maintain information security policies, procedures, and guidelines. • Provide guidance on data classifications			
Managers	▨	• Ensure users are aware of data classification requirements. • Monitor user activities to ensure compliance.		
Users	▨	• Identify data and label where appropriate. • Properly dispose of data in accordance with the records retention policy.		

Internal Communication and Reporting

[Below are two examples of how an initial notification of a cybersecurity incident may look. The first table-based example provides for consistent structure and form, while the second text-based example provides for a more comprehensive and adaptable approach.

At minimum, initial notification to management should provide a brief summary of the incident, focusing on business impacts, current and planned actions, and resources needed for resolution of the incident.

Both templates can be modified to suit your organization's needs. They can be used either individually or together.]

Table-Based Internal Management Cybersecurity Incident Alert

[Organization] Internal Cybersecurity Incident Alert	TLP: RED
Alert Date and Time	[Month DD, 20xx, 12:00 a.m. / p.m.]
Incident Name/Number	[Descriptive name or numbered naming convention]
Type	[Ransomware, Malware Infection, Data Breach, DDoS, or other attack type]
Incident Details	[Provide a summary (in less than 6 lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws (who, what, when, where, and why) and Impacts]
Public Impacts	[Status of Public Website, Payment Processing, Public Data Systems, Public Safety Answering Point, Supervisory Control and Data Acquisition (SCADA) Systems, or other public-facing system]
Internal Impacts	[Status of organization email, phone system, computer workstations, internal document and records storage, public safety, or other internal systems]
Current Containment Activities	
1. [List major activities taken to contain impacts] 2. 3.	
Planned Actions	
1. [List major actions planned to further contain and eradicate active threat] 2. 3.	
Supporting Actions or External Assistance Requests	
[List any supporting actions or external requests needed to facilitate incident response activities]	
Next Scheduled Update	[Month dd, 20xx at 12:00 a.m./p.m. or as conditions warrant]

Text-Based Internal Management Cybersecurity Incident Alert

Organization Information

Notification Made to

- [Name of person or team being notified]

Notification Made by

- [Name of person making the notification]

Incident Information

Type of Incident

- [Ransomware, malware infection, data breach, etc.]

Date and Time

- [MM/DD/YYY HH:MM AM/PM]

Incident Name/Tracking Number

- [Provide a short name for referencing the incident internally]

Incident Impact

- [Provide a brief list of internal processes or services that are impacted by this incident]
- [Provide a brief list of external processes or services that are impacted by this incident]

Executive Summary

- [Provide a brief summary (in less than six lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws and Impacts]

Incident Containment And Resource Management

Current Containment Action Items

- [Provide a brief list of major action items taken to contain the impact of the incident]

Planned Containment Action Items

- [Provide a brief list of planned action items for containing the impact of the incident]

Supporting Action Items

- [Provide a brief list of any supporting actions or external requests needed to facilitate incident response activities]

Next Steps

Next Notification Expected

- [MM/DD/YYY HH:MM AM/PM]

Daily Situational Report

[Leadership should receive consistent, frequent updates per your incident response plan’s reporting schedule.

Below are two examples of how a daily situational report notification for a cybersecurity incident may look. The first table-based example provides for consistent structure and form, while the second text-based example provides for a more comprehensive and adaptable approach.

At minimum, daily situational reports to management should provide a brief incident update, list any accomplishments, and focus on current and planned actions to resolve the incident.]

Table-Based Internal Management Daily Situational Report

[Organization] IRT Daily SitRep — Containment, Eradication, and Recovery	**TLP: AMBER**
Report Date and Time	[Month DD, 20xx, 12:00 a.m. / p.m.]
Incident Name/Number	[Descriptive name or numbered naming convention]
Current Priorities	[Current priority of incident response team]
BLUF	[(Bottom Line Up Front) – Define the most relevant activities associated with this report.]
Key Action Items	[Provide a summary of the progress made on each of the identified incident objectives or by organization unit, such as website restoration or application and developer activities.]
Accomplishments	
1. [List recent activities and progress made by the incident response team since the last report.] 2. 3. 4.	
Planned Activities/Next Steps	
1. [List the next planned activities to support incident response.] 2. 3. 4.	
Supporting Resources	
1. [List the internal and external resources (by group) supporting the incident response.] 2. 3.	
Next Scheduled Update	[Month DD, 20xx at 12:00 a.m./p.m. or as conditions warrant]

Text-Based Internal Management Daily Situational Report

Organization Information

Notification Made to

- [Name of person or team being notified]

Notification Made by

- [Name of person making the notification]

Report Information

Report Date and Time

- [MM/DD/YYY HH:MM AM/PM]

Incident Name/Tracking Number

- [Provide a short name for referencing the incident internally.]

Bottom Line Up Front (BLUF)

- [Provide a brief summary (in less than six lines) of the incident impacts. Include what happened, when it occurred, when and how it was discovered, and any additional high-level details appropriate for senior management notification. Consider using the 5 Ws and Impacts.]

Incident Containment And Resource Management

Accomplishments

- [Provide a brief list of action items accomplished in containing the impact of the incident.]

Planned Action Items

- [Provide a brief list of planned action items for containing the impact of the incident.]

Supporting Action Items

- [Provide a brief list of any supporting actions or external requests needed to facilitate incident response activities.]

Next Steps

Next Notification Expected

- [MM/DD/YYY HH:MM AM/PM]

Post-Incident After-Action Review and Improvement Plan

Post-Incident After-Action Review Report

[Use the sections below to capture post-incident comments captured in a hot wash or after-action review. Customize the content in brackets with your own details and information.]

Item	Description
Cyber Incident	[Use your organization's naming convention for the incident.]
Dates and Times	[Indicate, at a minimum, the start/end dates/times 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?]
Metrics	[Enter any related metrics such as mean time to incident discovery, cost of recovery, time from detection to containment, etc.]
Incident Cost	[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.]

Lessons Learned Questions

[The following table provides learning and improvement questions to assess the incident response.]

Question	Response
Were documented policies and procedures followed?	
Were the procedures adequate?	
Were all features, policies, and processes examined to identify all contributing factors that caused this incident?	
What information was needed sooner?	
Were any steps taken that might have inhibited recovery?	

Question	Response
What actions could the organization do differently if a similar incident occurs?	
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 or resources are needed to address future incidents?	

Root Cause Analysis Questions

[The following table provides questions for incident response root cause analysis.]

Question	Response
What could have prevented the incident?	
Was damage caused prior to detection?	
Is the incident a recurrence of a previous incident?	
Were all features, policies, and processes examined to identify all contributing factors that caused this incident?	

Question	Response
Was there a difference between the initial impact assessment and the final impact assessment?	
Were there any leading-edge indicators of detection that were missed?	

Response Strengths

[You can use this section to identify areas of the response that went well, including processes that worked as—or better than—intended and other strengths your organization identified during the response.]

[Our organization] identified these areas as strengths in our response to the incident. Strengths should be identified and captured as best practices.

Strength	Description

Response Improvement Opportunities

[Our organization] identified these areas for improvement in our response to the incident. Areas for improvement should be captured and analyzed to prevent the issue from recurring. Corrective actions for each area for improvement can be documented in the next section.

Area of Improvement	Description

Corrective Action Plan

This corrective action plan has been developed for [organization] because of the [incident name] Cyber Incident.

Improvement	Corrective Action	Responsible Stakeholder	Start Date	End Date	Notes or Limitations
[Improvement One]	[Corrective Action]	[Name/Org]	[MM/DD/YY]	[MM/DD/YY]	[As needed]
	[Corrective Action]				

Improvement	Corrective Action	Responsible Stakeholder	Start Date	End Date	Notes or Limitations
	[Corrective Action]				
[Improvement Two]	[Corrective Action]				
	[Corrective Action]				
	[Corrective Action]				
[Improvement Three]	[Corrective Action]				
	[Corrective Action]				
	[Corrective Action]				
[Improvement Four]	[Corrective Action]				
	[Corrective Action]				
	[Corrective Action]				
[Improvement Five]	[Corrective Action]				
	[Corrective Action]				
	[Corrective Action]				

Part Four - External Contacts and Resources

Part Four – External Contacts and Resources contains the contact information and resources available for external contacts. Collaboration with external entities may be necessary to assist with incident response or for auxiliary support. The response team shall ensure that all those participating in the incident response work together efficiently and effectively.

State of Texas Contacts

The following tables identify contact information for external partners within the state of Texas with whom the organization may collaborate in the event of an incident. Resource pages and other useful information are included.

Austin Police Department (APD) Digital Analysis Response Team (DART)

Conducts investigations of technology-related crimes in the City of Austin and helps other law enforcement agencies perform forensic examinations of digital evidence.

Contact	Email	Number
APD Main Line	Contact Us Form	(512) 974-5000
DART	-	(512) 974-8631

Office of the Attorney General (OAG)

The agency of the state's chief law enforcement official. Investigates cybercrime and provides computer forensics services to locate and preserve digital evidence. Protects Texas consumers by accepting complaints, filing civil cases in the public interest, and educating Texans on potential scams.

Contact	Email	Number
OAG Main Line	-	(512) 463-2100
Criminal Investigations Division	CJID@oag.texas.gov	(512) 936-1796

Resources

- Identity Theft Resources and Alerts
- Data Breach Reporting
- Criminal Investigations Division

State Auditor's Office (SAO) Special Investigations Unit

Investigates criminal offenses affecting state resources, including computer security.

Contact	Email	Number
SAO Special Investigations Unit Hotline	-	1 (800) 892-8348

Texas Department of Information Resources (DIR)

Provides information security services and communications technology services, including incident response and assistance, to Texas state agencies, local governments, public education entities, special districts, and more.

Contact	Email	Number
DIR Network Security Operations Center (NSOC) Analysis	security-alerts @dir.texas.gov	1 (888) 839-6762
DIR Security Hotline	DIRsecurity@dir.texas.gov	1 (877) 347-2476

Resources

- DIR Information Security Homepage
- DIR OCISO Security Services Guide

Texas Division of Emergency Management (TDEM)

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.

Contact	Email	Number
TDEM SOC	soc@tdem.texas.gov	(512) 424-2208

Texas Information Sharing and Analysis Organization (TX-ISAO)

Provides a mechanism for state and non-state entities in Texas to share actionable and timely information regarding cybersecurity threats, best practices, and remediation strategies. Available to Texas operations of public, private, and non-profit entities at no cost.

Resources

- TX-ISAO

Texas Secretary of State (SOS) Elections Division

Oversees the security policies of Texas elections. Report security incidents impacting election data to the election security point of contact.

Contact	Email	Number
SOS Elections Division	elections@sos.texas.gov	(512) 463-5650
SOS IT Security Officer	-	(512) 463-5683

Federal Contacts

The tables below identify federal contact information of external partners with whom the organization may collaborate in case of an incident. Resource pages and other useful information are included.

Cybersecurity and Infrastructure Security Agency (CISA)

Leads the national effort to understand, manage, and reduce risk to U.S. cyber and physical infrastructure.

Contact	Email	Number
CISA Central	central@cisa.gov	(888) 282-0870
Region 6	CISAregion6@hq.dhs.gov	-

Resources

- Incident Reporting Form (Including Phishing and Vulnerabilities)

Federal Bureau of Investigation (FBI)

Investigates high-tech crimes, including computer intrusions and theft of personal information.

Contact	Email	Number
Austin Resident Agency	-	(512) 345-1111
Dallas Field Office	-	(972) 559-5000
El Paso Field Office	-	(915) 832-5000
Houston Field Office	-	(713) 693-5000
San Antonio Field Office	-	(210) 225-6741

Federal Trade Commission (FTC)

Regulates consumer business practices.

Resources

- Recovering from Identity Theft

Office for Civil Rights (OCR), U.S. Department of Health and Human Services

Oversees federal civil rights and health information privacy, security, and breach notices required by the Health Insurance Portability and Accountability Act (HIPAA).

Resources

- OCR Home Page

U.S. Postal Service Inspector Service

Investigates crimes that may adversely affect or fraudulently use U.S. Mail, the postal system, or postal employees.

- Mail Fraud Complaint Form

U.S. Secret Service

Investigates financial crimes, including identity theft.

Contact	Email	Number
Dallas Field Office	-	(972) 868-3200
Houston Field Office	-	(713) 868-2299
San Antonio Field Office	-	(210) 308-6220

U.S. Treasury Inspector General for Tax Administration (TIGTA) and Office of Safeguards

Provides leadership and coordination, and recommends policy to promote economy, efficiency, and effectiveness in the administration of the internal revenue laws.

Contact	Email	Number
Dallas Field Office	-	(972) 308-1400

Industry Contacts

The tables below identify industry contact information of external partners with whom the organization may collaborate in case of an incident. Resource pages and other useful information are included.

American Health Information Management Association (AHIMA)

Contains information for health information management professionals with a useful resources page for health data.

- HIM's Role

Credit Bureaus

Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes.

Contact	Email	Number
Annual Credit Report	-	1 (877) 322-8228
Equifax	-	1 (877) 478-7625
Experian	-	1 (888) 397-3742
TransUnion	fvad@transunion.com	1 (800) 680-7289

Resources

- Annual Credit Report Home Page
- Equifax Home Page
- Experian Home Page
- TransUnion Home Page

Healthcare Information Management Systems Society (HIMSS)

Contains information related to health information management with resources page for health data.

- Cybersecurity in Healthcare

Payment Card Industry (PCI) Data Security Standards (DSS)

Contains payment card data security standards set by the payment card industry.

Resources

- PCI Security

Ponemon Institute

Conducts independent research on privacy, data protection, and information security policy.

- Ponemon Institute Home Page

Texas Media Directory

Contains distribution lists of Texas print and electronic media outlets.

- Texas Media Directory

Appendix A: Glossary and Acronyms

Glossary

The glossary below identifies terms and definitions relevant to cybersecurity.

Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or the identity confirmation process used to determine an individual's authorization to access data or computer resources.

Authorization

The act of granting a person or other entity permission to use data or computer resources in a secured environment.

Authorized User

A person granted certain permissions to access, manage, or make decisions regarding an information system or the data stored within the system.

Availability

The security objective of ensuring timely and reliable access to—and use of—information.

Breach

A verboten use or disclosure by an unauthorized person—or for an unauthorized purpose—that compromises the security or privacy resulting in the confirmed disclosure of data to an unauthorized party.

Breach of System Security

A breach involving electronic sensitive personal information (SPI) as defined by the Texas Identity Theft Enforcement and Protection Act, Business and Commerce Code Chapter 521 that compromises the security, confidentiality, or integrity of SPI. Breached SPI that is also Protected Health Information (PHI) may also be a HIPAA breach, to the extent applicable.

Chain of Custody

The application of the legal rules of evidence and its handling.

Confidential Information

(1) Information that must be protected from unauthorized disclosure or public release based on state or federal law, or other legal agreement, including any communication or record (whether oral, written, electronically stored, transmitted, or in any other form).

(2) Information identified in a contract or data use agreement that an organization contractor specifically seeks to obtain access for an authorized purpose that has not been made public.

Confidentiality

The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Containment

The process of preventing the expansion of any harmful consequences arising from an incident.

Disaster Recovery Plan

A crisis management master plan activated to recover IT systems in the event of a disruption or disaster. Once the situation is under control, a business continuity plan should be activated.

Discovery

The first time at which an event is known, or by exercising reasonable diligence should have been known, by an officer, director, employee, agent, or organization’s contractor, including events reported by a third party to an organization or organization’s contractor.

Encryption

The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Applicable law may provide for a minimum standard for compliant encryption, such as HIPAA or NIST standards.

Eradication

The removal of a threat or damage to an information security system.

Event

An observable occurrence in a network or system.

Forensics

The practice of gathering, retaining, and analyzing information for investigative purposes in a manner that maintains the integrity of the information.

Harm

(1) Although relative, the extent to which a privacy or security incident may cause damage to an organization.

(2) Damage to an individual’s reputation, finances, or identity.

Incident (or Security Incident)

An event that results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, exposure, or destruction of information or information resources.

Incident Response Lead

The person who is responsible for the overall information security incident management within an organization and for coordinating the organization’s resources to prevent, prepare for, respond to, or recover from an incident or event.

Incident Response Team (IRT)

Led by the incident response lead, the core team composed of subject-matter experts, information privacy staff, and security staff that aids in protecting the privacy and security of information that is confidential by law; provides a central resource for an immediate, effective, and orderly response to incidents at all levels of escalation.

Information Security

The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information Security Program

The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Integrity

The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Malicious Code

A software program that appears to perform a useful or desirable function but instead gains unauthorized access to computer system resources or deceives a user into executing other malicious logic.

Penetration

The unauthorized logical access to sensitive data by circumventing a system's protections.

Personally Identifiable Information (PII)

As defined by the Texas Business and Commerce Code Section 521.002(a)(1), "personally identifiable information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

- Name, social security number, date of birth, or government-issued identification number.
- Mother's maiden name.
- Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image.
- Unique electronic identification number, address, or routing code.
- Telecommunication access device as defined by the Texas Penal Code Section 32.51.

Privacy

The right of individuals to keep information about themselves to themselves and away from others. For example, privacy in the healthcare context means the freedom and ability to share an individual's personal and health information in private.

Protocol

A set of formal rules describing how to transmit data, especially across a network.

Recovery

The process of returning systems back to their pre-incident state to sustain normal business operations.

Reportable Event

An event that involves a breach of confidential information requiring legal notification to individuals, government authorities, the media, or others.

Risk Assessment

The process by which the potential for harm is identified and the impact of the harm is determined including the identification, evaluation, and documentation of the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems; incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Sensitive Personal Information (SPI)

As defined by the Business and Commerce Code section 521.002(a)(2), SPI means:

1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and items are not encrypted:
    - Social security number.
    - Driver's license number or government-issued identification number.
    - Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
2) Information that identifies an individual and relates to:
    - The physical or mental health or condition of the individual.
    - The provision of health care to the individual.
    - Payment for the provision of health care to the individual.

SPI does not include publicly available information that is lawfully made available to the public from the federal, state, or local government.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals by the unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Traffic Light Protocol (TLP)

The Traffic Light Protocol facilitates easier sharing of information. TLP is a set of "classifications" used to describe with whom sensitive information can be shared. TLP has four color designations and one color + modifier designation:

- TLP: RED - **Not for disclosure; restricted to participants only.**
- TLP: AMBER + STRICT - **Limited disclosure; restricted to participants' organizations.**
- TLP: AMBER - **Limited disclosure; restricted to participants' organizations or clients.**
- TLP: GREEN - **Limited disclosure; restricted to the community.**
- TLP: CLEAR - **Disclosure is not limited.**

Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Acronyms

The list of acronyms and descriptions below are commonly used in cybersecurity.

Acronym	Description
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 (2002)
FTI	Federal Taxpayer Information
HIPAA	Health Insurance Portability and Accountability Act (1996)
HITECH	Health Information Technology for Economic and Clinical Health Act (2009)
IRS	Internal Revenue Service
IRT	Incident Response Team
ISO	Information Security Office
NIST	National Institute of Standards and Technology
PHI	Personal Health Information
PIA	Public Information Act, Texas Gov't Code Ch. 552
PII	Personally identifiable information
SPI	Sensitive personal information
SSA	Social Security Administration
TAC	Texas Administrative Code
TLP	Traffic Light Protocol

DIR Disclaimer

Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any third-party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.

DIR OCISO

Office of the
Chief Information
Security Officer
State of Texas