Incident Response Team Redbook

Texas Department of Information Resources

Office of the Chief Information Security Officer

January 2022

**Table of Contents**

Introduction 1

Section 1: Incident Response Policy 2

1.1 Sample Security Incident Response Policy 2

Section 2: Privacy/Security Incident - Initial Triage Checklist 4

Section 3: Event Threat, Impact Analysis, and Escalation Criteria 5

3.1 Event Threat and Impact Analysis 5

3.2 Event Escalation: Communication 6

Section 4: Breach Notice Criteria 8

Section 5: Post-Incident Checklist 12

Section 6: Incident Response Team Templates 14

6.1 Title & Contact Information for Plan Sponsor/Owner 14

6.2 Incident Response Team Charter 15

6.3 IRT Membership by Roles 16

6.4 IRT State Government Contact Information 19

6.5 Services Restoration Priority Worksheet 20

6.6 Hardware and Software Inventory 21

Section 7: Additional Templates and Guidance 22

7.1 Public (Media) Notice 22

7.2 Identity Theft Protection Criteria 22

7.3 Notice to Individuals Affected by Incident 24

7.4 Post-Incident After Action Review and Improvement Plan 26

Section 8: External Contacts 30

Section 9: Legal References 35

9.1 Texas Laws and Regulations for Data Privacy and Security 35

9.2 Federal Laws and Regulations for Data Privacy and Security 38

9.3 Other Laws and Regulations for Data Privacy and Security 42

Acknowledgements 43

Appendix A: Additional Incident Response Team Templates 45

Appendix B: Texas Cybersecurity Program Best Practices 53

Appendix C: Glossary and Acronyms 60

Glossary 60

Common Acronyms 66

# Introduction

When a privacy or information security incident occurs, it is imperative that the organization follow documented procedures for responding to and processing the incident. An Incident Response Team (IRT) Redbook is intended to document the procedures and plans for such incidents. The Redbook should be maintained in both hard copy and electronic formats, readily available to any standing member of the IRT team.

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

The development of the Redbook is guided by two principles guide the development of the Redbook. First, every organization must pre-plan, develop and maintain an incident response plan. Second, every organization must test the operation and update the plan periodically to ensure its applicability.

This template is intended to be a framework for an organization to use while creating their own Redbook. It should be modified and completed to meet their specific business needs.

# Section 1: Incident Response Policy

Each organization should have a policy to address compliance with privacy and security incident management. Below is a sample policy, which organizations can customize by modifying the information in brackets [ ] to align the policy with the organization’s incident response plan.

## 1.1 Sample Security Incident Response Policy

The table below provides sample policy statements for the development of an organization’s incident response policy.

| Section | Guidance | |
| --- | --- | --- |
| **Purpose** | The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with [Texas Administrative Code (TAC), Title 1, Chapter 202](https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202). This document sets forth the policy for incident management within state level organizations but can be applicable to all organizations. | |
| **Scope** | This policy applies to any computing device owned or leased by the organization.  This policy applies to and must be complied with by all the organization’s users.  The user agrees to abide by this policy while employed or contracted with the organization.  Roles and responsibilities of each function pertaining to the protection of organization-owned systems and data are documented in the organization’s policy.  The user is responsible for understanding the terms and conditions of this policy. Exemptions to this policy shall follow the process defined in organization policy.  This policy is subject to change.  This policy applies to any computing device owned or leased by the organization. It also applies to any computing device regardless of ownership, which either is used to store organization-owned confidential or organization-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure. | |
| **Policy** | The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Information Resources Manager (IRM) for approval.  The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that fall under one of the following categories:  Propagation to external systems.  Violation of applicable federal and/or state laws which will require involvement from law enforcement.  Potential modification or disclosure of confidential information as defined in the Agency Data Classification Policy. | [1 TAC §202.26](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=26) |
| The agency shall notify appropriate individuals (which must include the state CISO and the state Cybersecurity Coordinator) within 48 hours if it is believed that personal information owned by the agency has been used or disclosed by or for unauthorized persons or purposes. | [TGC §2054.1125](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.1125) [TBC §521.053](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.053) |
| The ISO shall establish an Incident Criticality Matrix. This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants.  The ISO shall establish and document appropriate procedures, standards, and guidelines regarding incidents. | [1 TAC § 202.21](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=21)  [1 TAC § 202.22](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=22) |
| The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by the agency may be subject to seizure and retention by the ISO.  The Chief Information Security Officer, Chief Privacy Officer, or Agency General Counsel (as appropriate) will work directly with law enforcement regarding any incidents that may have violated federal or state laws. If an incident is determined to be the result of a privacy violation by a user, the ISO shall notify the user’s supervisor and Human Resources of the violation(s), or the Inspector General’s Office, as applicable, for appropriate action.  The ISO shall provide a summary report for each valid security incident to the IRM within five business days after the incident has been closed. | |
| **Disciplinary Action** | Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law.  Any user who has violated this policy may be subject to disciplinary action, up to and including termination of employment or contract with the organization.  The agency will cooperate with appropriate law enforcement if any user may have violated federal or state law. | |
| **Document Change Management** | All changes to this document shall follow the process defined in agency policy. | |
| The ISO will be responsible for communicating the approved changes to the organization. | [1 TAC § 202.21](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=21) |

# Section 2: Privacy/Security Incident - Initial Triage Checklist

The steps and potential actions identified below provide initial guidance when responding to a potential privacy/security event.

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

# Section 3: Event Threat, Impact Analysis, and Escalation Criteria

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

## 3.1 Event Threat and Impact Analysis

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

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

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

### Table 3.1: Examples of Functional Impact Thresholds

|  |  |
| --- | --- |
| **Threshold** | **Description** |
| **Catastrophic** | An incident meets the catastrophic threshold if it impacts multiple critical infrastructure systems including impacts to power generation and distribution, water and wastewater utilities, telecommunications, delivery of public health and medical services, government operations, public safety, or law enforcement information systems. |
| **Emergency** | An incident meets the emergency threshold if it impacts a single critical system, curtails delivery of public health and medical services, power generation and distribution, water and wastewater utilities, telecommunications, government operations, or public safety services. |
| **High** | An incident meets the high threshold if it results in noticeable impacts to government operations, public safety systems, or reduces public confidence in entities service delivery. |
| **Medium** | An incident meets the medium threshold if it results in the degradation of an organization’s program or services, or reduces public facing service delivery capacity |
| **Low** | An incident meets the low threshold if it impacts individual users or accounts. |

### Table 3.2: Explanations of Impact Terms

|  |  |
| --- | --- |
| **Category** | **Definition** |
| **Incident** | A security event that compromises the integrity, confidentiality, or availability of an information asset.[[1]](#footnote-2) |
| **Breach** | An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.1 |

### Table 3.3: Examples of Recoverability Effort Categories

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

## 3.2 Event Escalation: Communication

[NIST 800-61](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf) Computer Security Incident Handling Guide provides recommendations on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications. These and other relevant key contacts are listed below.

### Key Contacts

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

* Chief Executive Officer (CEO), Director, Commissioner, or Chief (as applicable)
* Chief Information Officer (CIO) or Information Resources Manager (IRM)
* Chief Information Security Officer (CISO) or Information Security Officer (ISO)
* Chief Privacy Officer (CPO) or Privacy Officer
* Chief Risk Officer (CRO) or Risk Manager
* Other incident response teams within the organization
* External (contractor) incident response teams, if appropriate
* System owner
* Internal departments, including human resources, public affairs, and legal
* (Local) Mayor or County Judge
* (Local) Emergency Management Coordinator
* (Local) Texas Division of Emergency Management (TDEM) District Coordinator
* (Local) Council of Government (COG) or Regional Planning Commission (RPC) 9-1-1 Administrator
* US-CERT (required for systems operated on behalf of the federal government)
* Law enforcement, if appropriate
* Federal government agencies, if appropriate
* Texas Information Sharing and Intelligence Organization (Texas ISAO)
* Additional Information Sharing and Intelligence Organizations (ISAO) (as appropriate)
* Department of Information Resources Office of the CISO (mandated for state agencies)

### Contact Methods

Organizations may need to provide status updates to certain external and internal parties during incident response. The list below identifies potential communication methods.

* Email updates
* Website (internal, external, or portal)
  + Note: The official state portal to notify DIR is SPECTRIM. All state level organization/agency ISOs have access to this system.
* Social media posts
* Alerting and Communication Systems (to deliver automated text or phone call)
* Telephone calls (call tree)
* In person (e.g., daily briefings)
* Voice mailbox greetings (e.g., set up a voice mailbox greeting for incident updates and update the greeting message to reflect the current incident status.)
* Paper (e.g., post notices in common areas and hand out notices at building entrance.)

# Section 4: Breach Notice Criteria

Certain types of breaches trigger legal notification responsibilities. This section includes information about breach notification statutes and rules according to Texas law, federal laws and regulations, and other states’ laws. **NOTE** As of September 1, 2019 [Texas Gov’t Code section 2054.1125](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.1125) requires notification of the Texas Office of the Chief Information Security Officer within 48 hours of discovery for all breaches (actual or suspected) which require disclosure by law or agreement. For any breach involving election data, the Office of the Secretary of State must be notified.

### Table 4.1: Texas legal requirements for breach notices

| **Type** | **Citation** | **Requirement** | **Notes** |
| --- | --- | --- | --- |
| Texas Identity Theft Enforcement and Protection Act (2019) | [Business and Commerce Code section 521.053](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.053) | Report any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person or to the data owner immediately. Public reports may be required for breaches involving 10,000 or more individuals.  An organization that is required to disclose or provide notification under this section, is required to notify the Texas Attorney General if the breach involves at least 250 Texas residents. This notification must include:  A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired because of the breach.  The number of residents of this state affected by the breach at the time of notification.  The measures taken by the person or organization regarding the breach.  Any measures the person or organization intends to take regarding the breach after the notification under this subsection.  Information regarding whether law enforcement is engaged in investigating the breach. | [Gov’t Code section 2054.1125](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.1125) makes Business and Commerce Code 521.053 applicable to state agencies.  [Texas OAG Data Security Breach Report Form](https://oagtx.force.com/datasecuritybreachreport/s/) |
| Texas Education Code - District Cybersecurity | [Texas Education Code section 11.175](https://statutes.capitol.texas.gov/Docs/ED/htm/ED.11.htm#11.175) | The district's cybersecurity coordinator shall report to the Texas Education Agency any cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident. | A breach of system security is defined as an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by an unauthorized person. |

### Table 4.2: Federal legal requirements for breach notices

| **Type** | **Citation** | **Requirement** | **Notes** |
| --- | --- | --- | --- |
| HIPAA | [45 CFR §164.404](http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-404.pdf) | Notify individual or covered entity of a breach of unsecured protected health information, which poses a significant risk of financial, reputational, or other harm to the individual.  Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach. | Applies only to HIPAA Covered Entities and HIPAA-protected health information. A business associate of a covered entity is required to notify the covered entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice. |
| Centers for Medicare & Medicaid Services (CMS) | [CMS SMDL #06- 022](http://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf) | CMS regulated entities must notify CMS within one clock hour according to September 2006 CMS letter to State Medicaid Directors. | Unclear if [HIPAA HITECH](https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html) eliminated the CMS requirement.  SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or recipient is limited to use or disclosure “directly in connection with program administration,” but have no breach notice requirement. |
| Internal Revenue Service (IRS) | By data sharing agreement with the IRS, pursuant to [IRS Publication 1075 §10](http://www.irs.gov/pub/irs-pdf/p1075.pdf) | Notify Treasury Inspector General for Tax Administration (TIGTA) and IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals. | The IRS Office of Safeguards may require individual notification. |
| Social Security Administration (SSA) | By contract between SSA and Agency which defers to [IRS Publication 1075](http://www.irs.gov/pub/irs-pdf/p1075.pdf) | Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any. | SSA may require individual notification. |
| Federal Trade Commission (FTC) | Health Breach Notification (PHR, HER Vendors) [16 CFR Part 318](http://www.gpo.gov/fdsys/pkg/CFR-2012-title16-vol1/pdf/CFR-2012-title16-vol1-part318.pdf) | Requires a vendor of personal health records to notify the individual US citizen and the FTC following the discovery of a breach of security of unsecured PHR-identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR-related entity.  Note: “Breach” is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60-calendar days after the breach discovery. | Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. |
| Family Educational Rights and Privacy Act (FERPA) (1974) | [20 USC § 1232g](https://dir1.sharepoint.com/sites/ciso/Shared%20Documents/Incident%20Response/Projects%20Routine/Plans%20and%20Documents/Redbook/2020%20Revision/Draft/of%20%20subparagraph%20%20(A)shall%20%20not%20%20operate%20%20to%20%20make%20%20available%20%20to%20%20studentsin%20%20institutions%20%20of%20%20postsecondary%20%20education%20%20thefollowing%20materials:(i)%20%20financial%20%20records%20%20of%20%20th)  [34 CFR Part 99](https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl) | None. FERPA guidance recommends having breach response plans. | Applies to educational institutions regarding the privacy of personally identifiable information contained in education records of students. Consent is generally required to disclose education records. |

### State Data Breach Notification Laws

The National Conference of State Legislatures (NCSL) maintains a [matrix of state data breach laws.](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx) As of April 2021, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

The NCSL state data breach law matrix is available at the link provided below.

<https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

### Table 4.3: Contracted Data Breach and Credit Monitoring Services

The Texas Comptroller of Public Accounts (CPA) Statewide Procurement Division (SPD) manages a contract for Data Breach and Credit Monitoring Services.

|  |  |
| --- | --- |
| Contracting Agency | [www.txsmartbuy.com](http://www.txsmartbuy.com) |
| Contract Description | Data Breach and Credit Monitoring Services |
| Contract Number | 961-C1 |
| Contract Link | <http://www.txsmartbuy.com/contracts/view/2192> |

# Section 5: Post-Incident Checklist

The Computer Security Incident Handling Guide ([NIST 800-61](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf)) provides guidance on event analysis activities. NIST 800-61 Sections 3.4.1 and 3.4.2 provide guidance for capturing lessons learned and using collected incident data for post-incident and root cause analysis, which include:

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

# Section 6: Incident Response Team Templates

This section provides templates that are relevant to the development and operation of an incident response team. The plan sponsor or owner is responsible for modifying these templates for the incident response team’s use. Brackets or light blue shading indicate where the templates should be customized to reflect the organization.

## 6.1 Title & Contact Information for Plan Sponsor/Owner

**[Organization Name]**

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

For questions or further information, please contact:

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Phone | Email |
| Sponsor\* |  |  |  |
| Owner\*\* |  |  |  |
| \*Sponsor is the executive responsible for compliance  \*\*Owner is the owner of this document | | | |

## 6.2 Incident Response Team Charter

### Charter Purpose

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

### IRT Mission

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

### Overview

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

### Responsibilities and Roles:

Responsibilities:

* **Anticipate and prepare** [the organization] for privacy or security events/incidents which can be reasonably anticipated.
* **Respond** to actual or suspected events/incidents on behalf of [the organization] as needed, with activities such as:
  1. Triage, (*see* SECTION 2: Privacy/Security Incident - Initial Triage Checklist).
  2. Track and document IRT activities and discoveries.
  3. Prepare post-event/incident analysis and lessons learned (*see* SECTION 5: Post-Incident Checklist).

Examples of significant events/incidents within IRT responsibility:

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

Roles:

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

## 6.3 IRT Membership by Roles

The following table contains contact information for current IRT members.

Keep in mind the following considerations:

* In some cases, a member listed below may have designated another organization employee to represent him or her.
* The IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.
* Standing IRT Membership contact information should remain confidential to protect member names and personal contact information.
  + Work phone numbers are not traditionally confidential.
* Standing members are relatively static; ad hoc members are designated for each incident.
* Valid after-hours contact information is critical to incident handling.

### Standing IRT Members

| Title | Name | Phone | Email | After-Hours Contact |
| --- | --- | --- | --- | --- |
| IRT Lead | Jane Smith | 512-555-5555 | Jane.Smith@email[.]com | 512-555-5555 |
| [Chief Information Officer or designee] |  |  |  |  |
| [Chief Information Security Officer or designee] |  |  |  |  |
| [Information Resources Manager or designee] |  |  |  |  |
| [Internal Audit] |  |  |  |  |
| [Office of Inspector General] |  |  |  |  |
| [Other] |  |  |  |  |
| [Other] |  |  |  |  |
| [Other] |  |  |  |  |
| Legal Counsel to the IRT – To avoid losing attorney-client privilege, do not list legal as a member |  |  |  |  |
| Last updated: mm/dd/yyyy | | | | |

### Ad Hoc IRT Members

| Title | Name | Phone | Email | After-Hours Contact |
| --- | --- | --- | --- | --- |
| [Relevant business area, department, division] | Jane Smith | 512-555-5555 | Jane.Smith@email[.]com | 512-555-5555 |
| [Communications] |  |  |  |  |
| [External Relations] |  |  |  |  |
| [Open Records] |  |  |  |  |
| [Third parties, e.g.,  contractor] |  |  |  |  |
| [Department of Information Resources designee] |  |  |  |  |
| [Counsel, Office of Attorney General] |  |  |  |  |
| [Vendor for Breach Management services] |  |  |  |  |
| [Law Enforcement] |  |  |  |  |
| [Outside legal counsel] |  |  |  |  |
| [Other] |  |  |  |  |
| [Other] |  |  |  |  |
| [Other] |  |  |  |  |
| Last updated: mm/dd/yyyy | | | | |

## 6.4 IRT State Government Contact Information

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Entity or Organization** | **Title, Dept., or Location** | **Name** | **Phone** | **Email** |
| **Office of the Governor** |  |  |  |  |
| **Office of the Lt. Governor** |  |  |  |  |
| **Office of the Speaker of the House** |  |  |  |  |
| **Texas Chief Information Security Officer** | DIR - OCISO | Nancy Rainosek | 1 (877) 347-2476 | DIRSecurity@dir.texas.gov |
| **[Organizational Board Chief Official]** |  |  |  |  |
| **[Organization Chief Official]** |  |  |  |  |
| **Texas Division of Emergency Management** | Assistant Chief |  |  |  |
| District Coordinator |  |  |  |
| State Operations Center (SOC) | Daily Ops | (512) 424-2208 | [soc@tdem.texas.gov](mailto:soc@tdem.texas.gov) |
| **Texas DPS and CJIS** | Regional Office |  |  |  |
| DPS Cyber |  |  |  |
| CJIS | DPS OIC | 1-800-638-5387 | [Stephen.Petty@dps.texas.gov](mailto:Stephen.Petty@dps.texas.gov) |
| **[Organization]** |  |  |  |  |
| **[Organization]** |  |  |  |  |
| **[Organization]** |  |  |  |  |
| Last updated: mm/dd/yyyy | | | | |

## 6.5 Services Restoration Priority Worksheet

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

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

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| Tier | Service/System | Function and Details | End User |
| 1 | Domain controllers | Authentication – Active Directory | Internal and External |
| 1 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 2 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 3 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 4 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 6.6 Hardware and Software Inventory

Tracking your organization’s IT resources, including computers, servers, mobile devices, IP phones, other internet connected devices, and approved and managed software. This inventory allows IT or your managed service provider to track devices to maintain and provides a starting point to prioritize disaster recovery efforts.

### Table 6.1 Hardware Tracking

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset Number** | **Current Status** | **Assigned Employee** | **Asset Type** | **Model** | **Manufacture** | **Serial Number** | **Location** | **Description** | **Date Issued/Returned** |
| *TX-###* | *Assigned* | *John Doe* | *Laptop* | *Model Name* | *Manufacture* | *XX###X* | *HQ Level 2* | *Main Device* | *xx/xx/xxxx* |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

### Table 6.2 Software Tracking

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Software Use** | **Name** | **Software Description** | **License Type** | **Version** | **Software Key** | **Date Purchased** | **Billing Cycle** |
| *End User* | *Adobe Lightroom* | *Photo Editor* | *Service* | *NA* | *In Console* | *xx/xx/xxxx* | *Billed Monthly* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

The Center for Internet Security (CIS) provides a hardware and software asset tracking spreadsheet at <https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/>.

# Section 7: Additional Templates and Guidance

This section includes additional guidelines and templates which may be of use to the Incident Response Team, including:

* Public and media notice guidelines.
* Identity theft protection criteria.
* Sample notice to individuals affected by incident.

The plan sponsor or owner is responsible for modifying these templates to fit the IRT’s purpose. Brackets indicate where the IR Lead should customize the template to reflect the organization’s needs.

## 7.1 Public (Media) Notice

If the organization decides to notify the public at large, the information in the notice should mirror the information contained in the breach notice to individuals affected (*see* Section 7.3 Notice to Individuals Affected by Incident).

Media notice may be legally required; (*see* SECTION 4: Breach Notice Criteria). A media notice should be developed through the organization’s usual public communication processes and contain the following information:

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

## 7.2 Identity Theft Protection Criteria

Although a state agency or other organizations is often not required to provide identity theft protection, each organization should evaluate the risks for both financial and medical identity theft. If the risk is deemed significant, the organization may consider this type of protection. In addition to deciding whether to provide the protection, an organization should consider an appropriate length of time to provide the protection. Ultimately, the decision to provide protection should be made at an executive level. Should an organization determine identity theft protection is appropriate, there are various types and level of protection to choose from on the market, including:

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

The Texas Comptroller’s Smart Buy program has a contracted vendor for Data Breach and Credit Monitoring Services. As noted, commercial identity theft protection varies in the means and extent of coverage. While some carriers offer compensation for expenses incurred because of theft, others simply provide credit monitoring and alerts to an individual in the event of unauthorized credit activity. In addition to assistance for affected individuals, breach management services can be procured to assist an entity responsible for a breach, as well as provide risk assessment, mitigation, or remediation services. As circumstances warrant, organizations may elect to procure commercially available identity theft protection or breach management services, particularly for high-profile events likely to lead to significant harm to impacted individuals, reputational harm, or cost to the entity.

Entities should consider the following criteria to determine whether to procure identity theft protection or breach management services:

1. Contract opportunities made available to state agencies by the Texas Comptroller for identity theft or breach management services (*see* Table 4.3: Contracted Data Breach and Credit Monitoring Services).
2. Contractual requirements imposed upon the vendor, contractor, or third party responsible for the breach to provide identity theft protection, breach management services to the organization, or any other indemnification or hold harmless contract provisions.
3. Degree and scope of the breach and the degree or type of risks to individuals, such as financial, reputational, or other harm (such as medical identity theft or criminal identity theft), dependent upon the various forms of identity theft.
4. The extent to which commercial services will be unable to detect or deter harm such as medical or criminal identity theft for the breach at issue.
5. No or low-cost measures available to impacted individuals to protect themselves, such as instituting a self-imposed credit fraud alert, requesting a credit freeze from one of the credit bureaus [*see* Credit Bureaus in Table 8.3: Industry Contacts], or filing a police report. Some options for impacted individuals include:
   1. A fraud alertwhich can help prevent an identity thief from opening additional accounts in a consumer’s name for 90 days, with the option to extend to one year.
   2. A security freeze, also known as a credit freeze, is a tool that lets consumer’s restrict access to their credit report. Without access, businesses or others who may use an individual’s credit file will be unable to access the file without the freeze being lifted.
   3. Contacting the Consumer Protection Divisionof the Texas Office of the Attorney General.
6. The ability to link the breach event to an identity theft event or other harm.
7. The cost to the organization or organization contractor for the provision of identity theft or breach management services.

## 7.3 Notice to Individuals Affected by Incident

[Date]

[Title] [First Name] [Last Name]  
[Address]  
[City], [ST] [Zip]

Dear [Title] [Last Name]:

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

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

We are committed to helping you safeguard your information. [<Agency> is providing you with free credit monitoring and identity theft services for one year. This service includes an insurance policy of up to $< \_\_> in identity theft coverage, a year of <name of Agency’s contracted Breach Management Vendor product> coverage, and a full-service identity restoration team to guide you through the recovery process if anyone tries to misuse your information. You must enroll to take advantage of this free service.] [Describe the enrollment process if not described elsewhere.]

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

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

* Contact one of the national credit reporting agencies below and ask for a fraud alert on your credit report. The agency will alert all other agencies. Remember to renew these fraud alerts every 90 days. The state does not have authority to do this for you, as the credit bureaus require your permission to set up the alerts.

| **Reporting Agencies** | **Address** | **Contact Information** |
| --- | --- | --- |
| **Equifax** | P.O. Box 740241  Atlanta, GA 30374 | [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com/)  Fraud Hotline (toll-free): 1-877-478-7625 |
| **Experian** | P.O. Box 2002  Allen, TX 75013 | [www.experian.com](http://www.experian.com/)  Fraud Hotline (toll-free): 1-888-397-3742 |
| **TransUnion** | P.O. Box 6790  Fullerton, CA 92834 | [www.transunion.com](http://www.transunion.com/)  Fraud Hotline (toll-free): 1-800-680-7289 Report fraud: [fvad@transunion.com](mailto:fvad@transunion.com) |

* The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You should contact each agency to determine if a child has a file or if the child’s information has been misused.
* Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.
* Monitor your [bank account activity / health care records / medical insurance company explanation of benefits] to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to your [bank / health care provider / health insurance company’s privacy officer].
* Report any suspicious activities on your [credit reports or bank account / health care or health insurance records] to your local police or sheriff’s office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.
* Learn about the Federal Trade Commission’s identity theft programs by visiting [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft) or by contacting the Federal Trade Commission’s toll-free Identity Theft helpline at 1-877-ID-THEFT (1-877-438-4339); TTY: 1-866-653-4261.
* [Enroll in free credit monitoring and identity theft services provided by the state. There is no cost to you for the service, but **you must enroll**. You can enroll online at or by contacting <Organization’s contracted Breach Management Vendor’s> Customer Care Center toll- free at <phone number>].
* [To **enroll your minor child**, please call <Organization’s contracted Breach Management Vendor’s> Customer Care Center at <phone number> to manually enroll them. **Child enrollments cannot be conducted online**.]
* Monitor the website at [Organization’s contracted Breach Management Vendor’s organization / Organization’s own site] for periodic updates.

Please be assured that we are committed to helping you protect your credit and identity and in ensuring that your information is safe and secure.

If you have any questions, please call [Organization contact] at [phone number] or contact by email at [email address].

Sincerely,

[Authorized signatory]

## 7.4 Post-Incident After Action Review and Improvement Plan

### Incident Post-Incident After Action Review Template

Use the sections below to capture post-incident comments captured in a hot-wash or after action review.

[Replace 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 e.g., mean-time-to-incident-discovery, cost of recovery, time from detection to containment, etc.] |
| Incident Costs | [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.] |

The following table provides learning and improvement questions to access the incident response.

| Questions | Response | Comments |
| --- | --- | --- |
| How well did the staff and management perform? |  |  |
| Were documented policies and procedures followed? |  |  |
| Were the procedures adequate? |  |  |
| Was the actual cause identified? |  |  |
| What information was needed sooner? |  |  |
| Were any steps taken that might have inhibited recovery? |  |  |
| What should/would staff/management do differently the next time a similar incident happens? |  |  |
| How could information sharing (in/out) with other organizations have been improved? |  |  |
| What corrective actions can prevent or lower the likelihood of similar incidents in the future? |  |  |
| What precursors or indicators of compromise should be watched in the future to speed up detection? |  |  |
| What additional tools and/or resources are needed to address future incidents? |  |  |
| What tools, processes, metrics, or resources could be in place and/or monitored to detect a similar incident sooner? |  |  |

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

| Questions | Response | Comments |
| --- | --- | --- |
| What could have prevented the incident? |  |  |
| Was there damage caused prior to detection? |  |  |
| Is the incident a recurrence of a previous incident? |  |  |
| Was the actual cause identified? |  |  |
| Was there a difference between the initial impact assessment and the final impact assessment? |  |  |
| Were there any leading-edge indicators of detection that were missed? |  |  |

The following section identifies areas of the response that went well, including processes that work or other strengths your organization identified during the response.

### Response Strengths

The organization identified these areas as strengths in their response to the event. Strengths should be identified and captured as best practices for future events.

|  |  |
| --- | --- |
| Strength | Description |
|  |  |
|  |  |
|  |  |
|  |  |

### Response Improvement Opportunities

The organization identified these areas for improvement in their response to the event. Areas for improvement should be captured and analyzed. Corrective actions for each area for improvement can be documented in the next section.

|  |  |  |
| --- | --- | --- |
| 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** |
| --- | --- | --- | --- | --- | --- |
| 1. [Improvement One] | 1.1 [Corrective Action] | [Name/Org] | MM/DD/YY | MM/DD/YY | [As Needed] |
| 1.2 [Corrective Action] |  |  |  |  |
| 1.3 [Corrective Action] |  |  |  |  |
| 1. [Improvement Two] | 2.1 [Corrective Action] |  |  |  |  |
| 2.2 [Corrective Action] |  |  |  |  |
| 2.3 [Corrective Action] |  |  |  |  |
| 1. [Improvement Three] | 3.1 [Corrective Action] |  |  |  |  |
| 3.2 [Corrective Action] |  |  |  |  |
| 3.3 [Corrective Action] |  |  |  |  |
| 1. [Improvement Four] | 4.1 [Corrective Action] |  |  |  |  |
| 4.2 [Corrective Action] |  |  |  |  |
| 4.3 [Corrective Action] |  |  |  |  |
| 1. [Improvement Five] | 5.1 [Corrective Action] |  |  |  |  |
| 5.2 [Corrective Action] |  |  |  |  |
| 5.3 [Corrective Action] |  |  |  |  |

# Section 8: External Contacts

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

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

### Table 8.1: State of Texas Contacts

| Resource | Services | Contact Information |
| --- | --- | --- |
| Austin Police Department 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. | Austin Police Department, main number: (512) 974-5000  DART: (512) 974-8631 |
| Office of the Attorney General (OAG) | The agency of the state’s chief law enforcement official. | OAG main number: (512) 463-2100 |
| Consumer Protection Division: Protects Texas consumers by accepting complaints, filing civil cases in the public interest, and educating Texans on potential scams. | Identity Theft Resources and Alerts [https://www.texasattorney general.gov/consumer- protection](https://www.texasattorneygeneral.gov/consumer-protection) |
| Data Breach Reporting [https://www.texasattorney general.gov/consumer-protection/data-breach-reporting](https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting) |
| Criminal Investigations Division: Investigates cybercrime and provides computer forensics services to locate and preserve digital evidence. | (512) 936-1796 [CJID@oag.texas.gov](mailto:CJID@oag.texas.gov) Cybercrimes: (512) 463-9570 [https://www.texasattorney general.gov/divisions/law-enforcement/criminal-investigations](https://www.texasattorneygeneral.gov/divisions/law-enforcement/criminal-investigations) |
| OAG General Litigation Division: Defends state agencies, elected and appointed officials, and state employees (in their official capacity) in civil litigation. | [https://www.texasattorney general.gov/divisions/general-litigation](https://www.texasattorneygeneral.gov/divisions/general-litigation) |
| State Auditor’s Office, Special Investigations Unit | Investigates criminal offenses affecting state resources, including computer security breaches. | Hotline:  1-800-892-8348 |
| Texas Department of Information Resources, Network Security Operations Center | Provides information security services and communications technology services, including Incident response and assistance, to Texas state agencies, local governments, public education entities, and special districts. | DIR NSOC: [Security-alerts@dir.texas.gov](mailto:Security-alerts@dir.texas.gov)  1 (888) 839-6762  Option 1: Network Option 2: Security |
| Texas Department of Information Resources, Office of the Chief Information Security Officer | Provides information security program guidance to the Texas public sector. Led by the State of Texas Chief Information Security Officer, | DIR Security Hotline: 877-DIR-CISO (877) 347-2476  Email: [DIRSecurity@dir.texas.gov](mailto:DIRSecurity@dir.texas.gov) |
| Texas Information Sharing and Analysis Organization (ISAO) | The Texas 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.  It is available to all Texas operations of public, private, and non-profit entities at no cost. | [ISAO.Texas.Gov](https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=169) |
| 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. | State Operations Center [soc@tdem.texas.gov](mailto:soc@tdem.texas.gov)  (512) 424-2208 |
| Texas Rangers, Texas Department of Public Safety | Responsible for major incident criminal investigations in Texas. | Austin Headquarters:  (512) 424-2160 [rangers@dps.texas.gov](mailto:rangers@dps.texas.gov) |
| Texas A&M University System, Statewide Cybersecurity Services | The Texas A&M University System (TAMUS), Statewide Cybersecurity Services (SCS) provides security, monitoring, and consulting services to public entities in Texas. | TAMUS, SCS Contact Information <https://it.tamus.edu/scs/>  (979) 234-0030 [scs@tamus.edu](mailto:scs@tamus.edu) |

### Table 8.2: Federal Contacts

| **Resource** | **Services** | **Contact Information** |
| --- | --- | --- |
| CERT Coordination Center (CERT/CC) | Federally funded CERT provides technical advice to federal, state, and local agencies on responses to security compromises. | CERT 24-hour hotline: (412) 268-7090 [forensics@cert.org](mailto:forensics@cert.org) |
| Cybersecurity & Infrastructure Security Agency | CISA is responsible for protecting the nation’s critical infrastructure from physical and cyber threats. | [www.cisa.gov](http://www.cisa.gov)  Report Incidents: <https://www.us-cert.gov/report> |
| Federal Bureau of Investigation (FBI) | Cyber-squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information. | Dallas Field Office: (972) 559 5000 El Paso Field Office: (915) 832-5000 Houston Field Office: (713) 93-5000 San Antonio Field Office: (210) 225-6741 |
| Federal Emergency Management Agency (FEMA) | Provides disaster response and recovery assistance. | 1-800-621-FEMA (3362) |
| Federal Trade Commission (FTC) | Regulates consumer business practices. | Detecting Identify Theft <http://www.ftc.gov/idtheft> |
| National Institute of Standards and Technology (NIST), US Dept. of Commerce | Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 ([FISMA, 44 USC § 3541, et seq.](https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/FISMA-final.pdf)). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government. | Main Office (301) 975-NIST [inquiries@NIST.gov](mailto:inquiries@NIST.gov) <http://www.nist.gov/index.html>  Publications: <http://csrc.nist.gov/publications/> |
| Office for Civil Rights (OCR), US Dept. of Health and Human Services | Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA. | <http://www.hhs.gov/ocr> |
| US Postal Service Inspector Service | The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees. | <https://www.uspis.gov/>  [Mail Fraud Complaint Form](https://ehome.uspis.gov/fcsexternal/default.aspx) |
| US Secret Service | Investigates financial crimes, including identity theft. | Dallas Field Office: (972) 868-3200 Houston Field Office: (713) 868-2299 San Antonio Field Office: (210) 308-6220 |
| US Treasury Inspector General for Tax Administration (TIGTA) and Office of Safeguards | Works with agencies to ensure that all appropriate actions are taken regarding federal tax information. | Dallas Field Division: (972) 308-1400 |

### Table 8.3: Industry Contacts

| **Resource** | **Services** | **Contact Information** |
| --- | --- | --- |
| American Health Information Management Association (AHIMA) | AHIMA is an association of health information management professionals with a useful resources page for health data. | [http://www.ahima.org/ resources/infocenter/psc.aspx](http://www.ahima.org/resources/infocenter/psc.aspx) |
| Credit Bureaus | Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes.  Consumers may request a 90-day fraud alert, with the option to extend for one year.  Consumers who have filed an identity theft report may also place an extended, seven-year, fraud alert on their credit file.  Fraud alerts will be communicated with the other two credit bureaus by the bureau you contacted.  A credit freeze must be requested from each bureau individually. | Equifax: P.O. Box 740241  Atlanta, GA 30374  Fraud Hotline: 1-877-478-7625 [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com)  Experian: P.O. Box 2002  Allen, TX 75013 Fraud Hotline:  1-888-397-3742 [www.experian.com](http://www.experian.com)  TransUnion P.O. Box 6790 Fullerton, CA 92834 Fraud Hotline: 1-800-680-7289 [www.transunion.com](http://www.transunion.com) [fvad@transunion.com](mailto:fvad@transunion.com)  Annual Credit Report Request Service P.O. Box 105281  Atlanta, GA 30348-5281  1-877-322-8228 [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) |
| Health Information Management Systems Society (HIMSS) | HIMSS is an association of health information management professionals with resources page for health data. | [http://www.himss.org/ResourceLi](http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266) [brary/ResourceDetail.aspx?ItemN](http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266) [umber=17266](http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266) |
| Payment Card Industry – Data Security Standards (PCI-DSS) | Payment card data security standards set by the payment card industry. | [https://www.pcisecuritystandards](https://www.pcisecuritystandards.org/security_standards/) [.org/security\_standards/](https://www.pcisecuritystandards.org/security_standards/) |
| Ponemon Institute | Conducts independent research on privacy, data protection, and information security policy. | <http://www.ponemon.org> |
| Texas Media Directory | Subscription service for distribution lists of Texas print and electronic media outlets | [http://www.texasmedia.com](http://www.texasmedia.com/) |

# 

# Section 9: Legal References

This section covers a list of federal and state laws establishing relevant standards for types of confidential data, including a summary, and a citation. The list is not comprehensive and is not a substitute for seeking competent legal counsel familiar with all laws, rules, and standards governing specific organizations. Please refer to legal counsel for other relevant laws.

## 9.1 Texas Laws and Regulations for Data Privacy and Security

| **Reference** | **Description** | |
| --- | --- | --- |
| Texas Public Information Act | The Public Information Act contains provisions pertaining to information disclosure, including: | |
| The agency may not withhold information, even confidential information, if requested by a legislator or the Legislature for legislative purposes. | [TGC § 552.008](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.008) |
| Information confidential by law is excepted from disclosure. Example: [TGC § 2059.055](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2059.htm#2059.055). | [TGC § 552.101](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.101) |
| Is this IRT Redbook subject to disclosure under the Public Information Act? Some possible exceptions to disclosure for all or part of the book: | |
| Employee home addresses, home phone numbers, social security numbers, and family information is exempted from disclosure if the employee did not choose to disclose under §522.024, which may apply to IRT contact information.  Note: employee home email addresses possibly also excepted under 552.117. Unresolved issue: disclosure of employee work email address (otherwise public) may reveal who is on IRT. | [TGC § 552.117](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.117%27) |
| Network security is exempted from the requirement to disclose in the Public Information Act. | [TGC § 552.139](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.139), [TGC § 2054.055](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.055), [ORD 581 (1990](https://www.texasattorneygeneral.gov/sites/default/files/ord-files/ord/2020/ord19900581.pdf)) |
| Are records relating to the breach itself and the agency’s response confidential? Possible exceptions to disclosure include: | |
| Some personnel information may be private if in the personnel file; some transcripts are exempt from disclosure. | [TGC § 552.102](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.102), [TGC § 552.024](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.024), [TGC § 552.117](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.117) |
| Information related to litigation, if pending or reasonably anticipated, is exempt from disclosure. | [TGC § 552.103](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.103) |
| Information related to competition or bidding, generally while bidding is in process, is exempt from disclosure. | [TGC § 552.104](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.104), [TGC § 552.128](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.128) |
| Information submitted by a potential vendor or contractor is also exempted from disclosure. | |
| Attorney-client privilege and court-ordered confidentiality can be used to keep certain information from disclosure, with some limitations (*see* [TGC § 552.022(b)](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.022)). | [TGC § 552.107](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.107), [TGC § 552.022(b)](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.022) |
| Certain law enforcement records may be kept private, generally while the case is pending. |  |
| Trade secrets are exempt from public disclosure. | [TGC § 552.108](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.108) |
| Agency memoranda which would not be made available to a party in litigation (including attorney work product) are exempt from disclosure. | [TGC § 552.111](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.111) |
| Credit and debit card numbers as well as access device numbers may be kept from disclosure; additionally, according to ORD 684 (2009), insurance policy numbers, bank account numbers, and bank routing numbers can also be withheld from disclosure. | [TGC § 552.136](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.136), [ORD 684 (2009)](https://www.texasattorneygeneral.gov/sites/default/files/ord-files/ord/2020/ord20090684.pdf) |
| Email addresses of the public are exempt from disclosure. | [TGC § 552.137](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.137) |
| Social security numbers are exempt from disclosure. | [TGC § 552.147](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.147) |
| Note: the information that was the subject of the breach is also presumed to be protected from disclosure, possibly under sections not cited above. Each agency should be aware of how its own information is protected under the Public Information Act. | |
| With a few exceptions, agencies must receive a decision from the Office of the Attorney General before it can withhold information from a PIA request. The PIA contains some pitfalls, including some very strict deadlines. All agencies should consult an attorney or PIA coordinator for further guidance. | |
| Privacy Policy Necessary to Require Disclosure of SSN | A person may not require an individual to disclose one’s social security number to obtain goods or services from or enter into a business transaction with the person unless the person adopts a privacy policy, makes the policy available to the individual, and maintains the confidentiality and security of the social security number. The statute also prescribes required elements of a privacy policy. | [BCC § 501.052](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.501.htm#501.052) |
| Texas Identity Theft Enforcement and Protection Act | The Texas Identity Theft Enforcement and Protection Act requires notification to customers in the event of a security breach of customer’s computerized data, specifically customer’s personally identifiable information (PII).  The notification must be done as quickly as possible. The Act does provide for remedies not to exceed $50,000 per violation. If more than 10,000 individuals were affected by a breach, consumer reporting agencies must be notified. The Act does have a safe harbor when data is protected with encryption.  An organization that is required to disclose or provide notification under this section is required to notify the Texas Attorney General if the breach involves at least 250 Texas residents. This notification must include:  A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired because of the breach.  The number of residents of this state affected by the breach at the time of notification.  The measures taken by the person regarding the breach.  Any measures the person intends to take regarding the breach after the notification under this subsection.  Information regarding whether law enforcement is engaged in investigating the breach. | [BCC Ch. 521](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm)  [TGC § 2054.1125](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.2054.htm#2054.1125) |
| Texas Medical Records Privacy Act | The Texas Medical Records Privacy Act is Texas law making protected health information (PHI) confidential. This law is applicable to “Texas covered entities” or “any person who… comes into possession of protected health information,” a term more broadly defined than HIPAA’s “Covered Entities” and “Business Associates” (collectively: healthcare providers, healthcare clearing houses, health plans, and any business associates of the aforementioned). | [HSC Ch. 181](http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm) |
| Texas Administrative Code | Information Security Standards for state agencies and institutions of higher education. | [1 TAC 202](https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202) |
| Administrative rule pertaining to agencies’ websites. | [1 TAC 206](https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=206) |
| Each agency and institution of higher education must protect the privacy and personal identifying information (PII) of a member of public who provide or receive information from or through the institution’s website. Prior to providing access to information or services on a state website that requires PII, each institute must conduct a transaction risk assessment and implement appropriate safeguards that conform to TAC 202. | [1 TAC § 206.52](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=206&rl=52)  [1 TAC § 206.72](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=206&rl=72) |
| Texas rule in line with HIPAA, Privacy of Health Information, etc., provides for the privacy of health information, an individual’s right to correct such information, and the process for doing so. | [25 TAC § 1.501](https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=1&rl=501) |
| Cloud Computing State Risk and Authorization Management Program (TX-RAMP) | A state of Texas risk and authorization management program that provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. | [TGC § 2054.0593](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm#2054.0953) |

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

| **Reference** | **Description** | |
| --- | --- | --- |
| Health Insurance Portability and Accountability Act (HIPAA) (1996) | The Public Information Act contains provisions pertaining to information disclosure: | [HIPAA (1996)](http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html) |
| Privacy Rule: protects the privacy of individually identifiable health information.  Security Rule: sets national standards for the security of electronic protected health information.  Breach Notification Rule: requires covered entities and business associates to provide notification following a breach of unsecured protected health information.  Enforcement: providing civil and criminal penalties for violation.  Patient Safety Rule: protects identifiable information being used to analyze patient safety events and improve patient safety. | |
| Health Information Technology for Economic and Clinical Health Act (HITECH) (2009) | HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA business associates and requiring covered entities and business associates to report data breaches to those affected individuals through specific breach notification requirements. | [HITECH (2009)](http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf) [(ARRA Title XIII)](http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf) |
| HIPAA Omnibus Regulations (2013) | These regulations made substantial changes to HIPAA:  The Omnibus Regulations finalized the interim HITECH regulations.  Made business associates directly liable for certain privacy and security requirements.  Enacted stronger prohibitions on marketing (opt-out) and sale of Protected Health Information (PHI) without authorization.  Expanded individuals’ rights to receive electronic copies of PHI.  Allowed individuals the right to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full.  Required Notice of Privacy Practices updates and redistribution.  Changed authorization related to research and disclosure of school proof of child immunization and access to decedent information by family members or others.  Enhanced enforcement in many ways, including addressing the enforcement against noncompliance with HIPAA Rules due to willful neglect.  Finalized the rule adopting changes to the HIPAA Enforcement Rule to incorporate tiered, mandatory penalties up to $1.5 million per violation.  Finalized rule adopting GINA and prohibited most health plans from using or disclosing genetic information for underwriting purposes, as proposed in October 2009. | [45 CFR Parts 160-164](http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf) |
| Family Educational Rights and Privacy Act (FERPA) (1974) | FERPA creates a right of privacy regarding grades, enrollment, and billing information. Specifically, this information may not be released without prior consent from the student. In addition to safeguarding individual student records, the law also governs how state agencies transmit testing data to federal agencies. | [20 USC § 1232G](http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf) [34 CFR Part 99](http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf) |
| Federal Information Security Management Act (FISMA) (2006) | Federal legislation that assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to provide for the strengthening of information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to effectively and efficiently drive down IT security issues to acceptable levels through a defined framework by which federal government agencies would ensure the security of information systems controlled by either the agency or one of its contractors on behalf of a federal agency. The framework is further defined by the standards and guidelines set forth by NIST. | [44 USC §§ 3541-3549](http://csrc.nist.gov/drivers/documents/FISMA-final.pdf) |
| Internal Revenue Service Statute and Regulation | Through Publication 1075, the IRS has created a framework by which Federal Tax Information (FTI) and Personally Identifiable Information (PII) is protected from public disclosure. To ensure the safety of such data, receiving agencies and/or entities must have proper safeguards in place. Federal code requires external agencies and other authorize recipients of federal tax return and return information (FTI) to establish specific procedures to ensure the adequate protection of the FTI they receive. In addition, the same section of the code authorizes the IRS to suspend or terminate FTI disclosure to a receiving agency or other authorized recipient if misuse or insufficient FTI safeguards are found. In addition to criminal sanctions, the Internal Revenue Code prescribes civil damages for unauthorized disclosure and, when appropriate, the notification to affected taxpayers that an unauthorized inspection or disclosure has occurred. | [Publication 1075](http://www.irs.gov/pub/irs-pdf/p1075.pdf);  [IRC Section](http://www.law.cornell.edu/uscode/text/26/6103) [6103(p)(4](http://www.law.cornell.edu/uscode/text/26/6103));  [26 USC](http://www.law.cornell.edu/uscode/text/26/6103) [§6103(p)(4)](http://www.law.cornell.edu/uscode/text/26/6103) |
| Social Security Administration (SSA) Statute and Regulation | Much of the information SSA collects and maintains on individuals is especially sensitive. Therefore, prior to disclosing such information, SSA must look to the Privacy Act of 1974, 5 USC Section 552a, FOIA, 5 USC Section 1106 of SSA, 42 USC Section 1306. SSA employees are prohibited from disclosing any information contained in SSA records unless disclosure is authorized by regulation or otherwise required by federal law. SSA may only disclose personal records (PII) when the individual to whom the record pertains provides written consent or when such disclosure falls into one of the several narrowly drawn exceptions. | [Privacy Act of](http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf) [1974](http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf);  [5 USC Section 552a](http://www.law.cornell.edu/uscode/text/5/552a);  [FOIA](http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm);  [5 USC §1106 (SSA)](http://www.socialsecurity.gov/OP_Home/ssact/title11/1106.htm);  [42 USC §1306](http://www.gpo.gov/fdsys/granule/USCODE-2010-title42/USCODE-2010-title42-chap7-subchapXI-partA-sec1306/content-detail.html) |
| National Institute of Standards and Technology (NIST) | NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and to help with managing cost effective programs to protect their information systems and the data stored on the systems. NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in FIPS 200. The security rule covers 17 areas, including control, incident response, business continuity, and disaster recoverability. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls. Agencies are expected to comply with NIST security standards and guidelines. | [NIST 800-53  rev. 4](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf);  [FIPS 200](http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf) |
| Criminal Justice Information Services (CJIS) | CJIS is a division of the FBI that compiles data provided by law enforcement agencies across the United States. CJIS is the world’s largest repository of criminal fingerprints and history records which can be accessed and searched by law enforcement to enable the quick apprehension of criminals. The responsibility of CJIS extends to the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Incident-Based Reporting System (NIBRS). In addition to its many responsibilities in the coordination and sharing of criminal data, CJIS promulgates the CJIS Security Policy, which is meant to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI).  The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. The policy applies to every individual – contractor, private entity, noncriminal justice agency representatives, or members of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information. | [CJIS Security Policy](http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)  [TGC § 552.108](http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm#552.108) |
| Clinical Laboratory Improvements Amendments (CLIA) | CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services. | [CLIA Regulations and Guidance](https://www.cdc.gov/clia/law-regulations.html) |
| Computer Fraud and Abuse Act (CFAA) | CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines “protected computers” as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication. | [18 USC §1030](https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf) |

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

| **Reference** | **Description** | |
| --- | --- | --- |
| General Data Protection Regulation (GDPR) (2018) | The General Data Protection Regulation (GDPR) is a privacy and security law drafted and passed by the European Union (EU). It imposes obligations onto organizations across the globe, so long as they target or collect data related to people in the EU.  The GDRP includes many key regulatory points, including data protection principles, accountability, data security, data protection by design and by default, when data can be processed, consent, data protection officers, and privacy rights. | [GDPR (2018)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679) |

# Acknowledgements

Incident Response Team Redbook was published on behalf of the Department of Information Resources, with the input of the Statewide Information Security Advisory Committee (SISAC), Privacy Advisory Committee, Data Breach Response Subcommittee. The members included:

|  |  |  |
| --- | --- | --- |
| **Committee** | **Name and Title** | **Organization** |
| Co-Chair | Sheila Stine, JD - Chief Privacy Officer (former) | Health and Human Services Commission |
| Co-Chair | Martin Zelinsky, JD General Counsel (former) | Department of Information Resources |
| Member | Chad Lersch, JD Assistant General Counsel (former) | Department of Information Resources |
| Member | Betsy Loar, JD Assistant Commissioner and General Counsel (former) | Credit Union Department |
| Member | Shelley Janda, JD Assistant General Counsel (former) | Department of Aging and Disability Services |
| Member | Susan Maldonado, JD Assistant General Counsel (former) | Texas Facilities Commission |

Members’ participation in creating this document is appreciated. The 2021 update of the DIR Redbook was published by the Department of Information Resources, with the input of the Statewide Incident Response Working group. The members include:

| **Organization** | **Name** | **Title** |
| --- | --- | --- |
| Texas Department of Information Resources | Nancy Rainosek | CISO, State of Texas |
| Andy Bennett | Deputy CISO, State of Texas (Former) |
| Brian Acklen | DCS ISO, STS Security Program Manager |
| Daniel Hankins | Cybersecurity Coordinator (Former) |
| Jonathan King | Incident Response and Resilience |
| Meredith Noёl | Cybersecurity Coordination Program Manager |
| Jeremy Wilson | Deputy CISO, Security Operations/CIRT |
| Texas Military Department | LTC Michael Reed | J6 - Deputy Director, CIO |
| Capt Nathaniel Bell | Cyber Response Coordinator |
| Col Christopher ‘Kit’ Howell | Cyberspace Operations Division Chief |
| LTC Chris Winnek | Deputy CIO - Cyber Chief |
| MAJ Matt Marty | Cyberspace Operations Branch Chief |
| Texas A&M University System | Dan Basile | Executive Director |
| Texas Department of Public Safety | Aaron Blackstone | Chief Information Security Officer |
| Mike George | Senior Strategic Planner |
| John Nichols (Maj Gen Ret.) | Strategic Planner |
| Brandon Gentry | Strategic Planner |
| Texas Division of Emergency Management | Lana Johnson | Planner II, Operational Planning Unit |

# Appendix A: Additional Incident Response Team Templates

This section provides additional templates to support the formation of an incident response team and their operation during a security incident.

## Incident Response Team: Meeting Agenda

|  |  |  |  |
| --- | --- | --- | --- |
| Meeting Agenda for [Organization] IRT Meeting | | | **TLP:GREEEN** |
| **Planned Meeting Date and Time** | | Month DD, 20xx, 12:00 a.m. / p.m. | |
| **Purpose**: This meeting agenda identifies the date and time, participants, and planned discussion topics for the organization’s incident response team. | | | |
| IRT Members Invited |  | | |
| **Ad Hoc IRT Members Invited** |  | | |
| **Invited Guests** |  | | |
| **Meeting Goals** | Summary of the meeting’s goals, items for discuss, and any topics on which members or guests should be prepared to present. | | |
| **Meeting Agenda** | | | |
| **Welcome and Introduction**   * Roll call/sign in * New member and guest introductions   **Follow up from last meeting**   * Meeting notes review * Holdover items   **Discussion Topic 1**   * Topic 1 Sub Item * Topic 1 Sub Item   **Discussion Topic 2**   * Topic 2 Sub Item * Topic 2 Sub Item   **Closeout**   * Announcements * Action Item Recap | | | |
| **Virtual Meeting Access** | Meeting URL:  Dial-in Phone Number:  Access Code: | | |

## Incident Response Team: Meeting Notes

|  |  |  |
| --- | --- | --- |
| Meeting Notes for [Organization] IRT Meeting | | **TLP:GREEEN** |
| **Meeting Date and Time** | Month DD, 20xx, 12:00 a.m. / p.m. | |
| **Purpose**: These meeting minutes document the participants, updates, and next steps when developing the organizations incident response capability. | | |
| IRT Members Present |  | |
| **Ad Hoc IRT Members Present** |  | |
| **Invited Guests** |  | |
| **Meeting Summary** | Summary of the meeting’s objectives, key points covered, and decision made. | |
| **Project Updates** | | |
|  | | |
| **Discussion Overview** | | |
|  | | |
| **Action Items** | | |
|  | | |
| **Next Scheduled Meeting** | Month DD, 20xx, 12:00 a.m. / p.m. | |

## Initial Internal Management Security Incident Alert Template

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Organization] Internal Data Security 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 W’s and Impacts] | | | |
| Public Impacts | [Status of Public Website, Payment Processing, Public Data Systems, Public Safety Answering Point, 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] | | | | |
| Planned Actions | | | | |
| 1. [List major actions planned to further contain and eradicate active threat] | | | | |
| Supporting Actions or External Assistance Requests | | | | |
| 1. [List any supporting actions or external requests needed to facilitate incident response activities] | | | | |
| Next Scheduled Update | | | Month dd, 20yy at 12:00 a.m./p.m. or as conditions warrant. | |

## Incident Response Team: Response Activity Coordination Toolkit

During incident response activities, managing and tracking the team member activities can be a challenge for incident commanders, team managers, and technical staff.

These three documents provide a method to track major issues and the command goals to address the identified issues, and the associated tasks down to the technical staff positions.

The purpose of each document is listed below.

* Incident Response Team - Issues and Goals List  
  *Identifies the major issues found by incident response team leadership and establishes goals to address these issues. These goals can then be assigned as actions to the IRT members using the Incident Response Team - Action Tracking List form.*
* Incident Response Team - Action Tracking List  
  *Provides incident response managers a system to track the activities assigned to incident response team members and to recognize their progress on the actions which support response goals.*
* Incident Response Team - Member Activity Tracking Log  
  *Provides a standardized tracking log for team members to document their activities in support of each action identified by incident response management during each shift.*

The graphic below provides a visualization of these forms’ intended use.



## Incident Response Team: Issues and Goals List

|  |  |  |
| --- | --- | --- |
| [Organization] Incident Response Team Action Tracking List | | **TLP:AMBER** |
| **Current Updates as of** | Month DD, 20xx, 12:00 a.m. / p.m. | |
| **Incident Name** | [Incident Name] | |
| **Purpose**: Identifies the major issues found by incident response team leadership and establishes goals to address these issues. These goals can then be assigned as actions to the IRT members using the Incident Response Team - Action Tracking List form. | | |

| **Item** | **Issue** | **Goal** | **Goal Date** |
| --- | --- | --- | --- |
|  | [Organization Website Is Down] | [Re-establish website access for users] | 5/8/2021 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Incident Response Team: Action Tracking List

|  |  |  |
| --- | --- | --- |
| [Organization] Incident Response Team Action Tracking List | | **TLP:AMBER** |
| **Current Updates as of** | Month DD, 20xx, 12:00 a.m. / p.m. | |
| **Incident Name** | [Incident Name] | |
| **Purpose**: This from provides incident response managers a system to track the activities assigned to incident response team members and to recognize their progress on the actions which support response goals. | | |

| **Item** | **Goal** | **Actions** | **Order, Priority, or Dependency** | **Assigned To** | **Status** |
| --- | --- | --- | --- | --- | --- |
|  | [Re-establish Website] | Rebuild IIS and SQL Server. | NA | Member 1 | In-Progress |
|  | [Re-establish Website] | Migrate and reload web content. | Goal 1.2 | Member 1 | Pending #1 |
|  | [Re-establish Website] | Configure and test website. | Goal 1.3 | Member 2 | Pending # 2 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Incident Response Team: Member Activity Tracking Log

|  |  |  |
| --- | --- | --- |
| [Organization] Incident Response Member Action Tracking Log | | **TLP:AMBER** |
| **Operational Period** | MM/DD/YY 12:00 a.m. / p.m. to MM/DD/YY 12:00 a.m. / p.m. | |
| **Incident Name** | [Incident Name] | |
| **Purpose**: This form provides a standardized tracking log for team members to document their activities in support of each action identified by incident response management during each shift. | | |

| **Item** | **Time** | **Action** | **Notes** | **Status** |
| --- | --- | --- | --- | --- |
|  | 0900 | [Rebuild IIS and SQL Server] | [Enter notes about tasks associated with this action] | In-Progress |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Incident Response Team: 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 First – Define the most relevant activities associated with this report.] | | | | |
| **Key Activities** | [Provide a summary, of the progress made on each of the identified incident objectives or by organization unit. i.e., website restoration, or application and developer activities] | | | | |
| **System Recovery Status** | [Status of organization’s major systems by percent restored, estimated restoration time or another identified metric] | | | | |
| **Accomplishments** | | | | |
| 1. [List recent activities and progress made by the incident response team since the last report] | | | | |
| **Planned Activities/Next Steps** | | | | |
| 1. [List the next planned activities to support incident response] | | | | |
| **Supporting Resources** | | | | |
| 1. [List the internal and external resources (by group) supporting the incident response] | | | | |
| **Next Scheduled Update** | | Month dd, 20yy at 12:00 a.m./p.m. or as conditions warrant. | | |

# 

# Appendix B: Texas Cybersecurity Program Best Practices

This appendix provides a set of cybersecurity tasks and considerations an organization may consider when implementing a cybersecurity program. Each task and associated considerations are mapped to the phases of the [Texas Cybersecurity Framework](https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Framework%20Controls%20and%20Definitions.pdf), a document that helps organizations track security controls and measures to an identified best practice.

While there is no single way to build a security program, organizations may evaluate the following tasks, considerations, and resources to facilitate its development.

The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any 3rd 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.

## Tasks and Considerations

The framework is divided into five phases, which are listed in the graphic below. To support organizations just starting a cybersecurity program, the ‘Setting up For Success’ section includes some tasks and considerations that may help you initiate a program. To help maintain a program, the “Supporting Long-term Success” section has suggested tasks and considerations.

### The suggestions are not intended to be all encompassing and each organization should consider their own risk level, funding, and priorities while implementing a security program. After reviewing this appendix, you should be able to identify tasks and supporting resources to help develop your organization’s cybersecurity program.

### Setting up For Success

These tasks may help establish a foundation on which entities can build a cybersecurity program and support continuous improvement.

|  |  |
| --- | --- |
| **Task** | **Considerations** |
| **Identify a cyber champion** | * explain the benefits of cybersecurity to leadership to gain support - cybersecurity manages information risk to an acceptable level to meet organizational goals * communicate risks and cybersecurity posture to leadership * advocate for security initiatives and priorities, based on risk appetite * develop metrics to evaluate and guide program |
| **Establish a cyber aware culture** | * train users on security policies including how to report suspicious emails or activity * develop a schedule for security activities, to continually engage users * host Cybersecurity Awareness Month events * consider implementing a reward system |

### Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

|  |  |
| --- | --- |
| **Task** | **Considerations** |
| **Inventory systems and their associated data** | * identify critical business functions * identify people/information/technology/facilities that support critical functions * determine the criticality and sensitivity of data, and the system(s) in which the data reside * document and maintain a network architecture diagram |
| **Perform a security assessment** | * adopt a cybersecurity framework * schedule and conduct a cybersecurity assessment (internal and conducted by a 3rd party) to measure current state and identify gaps * develop a roadmap to address gaps (aligned with business objectives) * share results with senior leadership and cyber champion * repeat assessment yearly to measure progress * consider having network and web-based applications penetration tested |
| **Develop security polices and document processes** | * develop and routinely update security policies that align with the organization’s security priorities * seek executive management endorsement of security policies * mature the processes and procedures used to protect critical systems |
| **Develop security staff skillsets** | * identify skills needed to support the cybersecurity program * assess if staff have the necessary skills * prioritize training to address any gaps, or consider leveraging external resources |

### Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

| **Task** | **Considerations** |
| --- | --- |
| **Implement a password policy** | * define complexity and rotation requirements * enable Multi-Factor Authentication, if possible, especially for critical systems, remote network access, and administrative access accounts * disable default service accounts on enterprise assets * incorporate screen locks |
| **Implement, protect, and test back-ups and data** | * implement a schedule to perform frequent (ideally automated) back-ups, prioritizing critical systems and data * maintain back-ups offline, and if possible, offsite * implement risk-based protections for offline back-ups * test back-ups regularly * retain data according to data management processes, securely storing and destroying data when no longer required * protect system logs from attackers |
| **Implement an Access Control and Account Management policy** | * develop a process for requesting, creating, issuing, modifying, and disabling/revoking user accounts, and consider automating the process * determine how to approve access to resources and applications (least privilege) including conditions for access group and role membership * remove local admin rights from standard users and actively monitor privileged accounts |
| **Control Oversight and Safeguard Assurance** | * review current tools to determine capability, correct configuration, and the level of support provided by each tool’s vendor * restrict allowable applications for end users to authorized and supported software for official work functions * encrypt sensitive data at rest and in transit * consider blocking macros in Office documents and other unnecessary file types |
| **Train end users on security awareness** | * develop a policy to ensure security awareness training is provided to all users (including managers, senior executives, and contractors) and incorporates the criteria from Texas Government Code 2054.519(b) * consider incorporating role-based security training to personnel with assigned security roles and responsibilities |
| **Implement personnel and third-party security requirements** | * screen employees and contractors * incorporate escalating levels of scrutiny based on roles and data that they will have access to * conduct background checks as appropriate, or as required by law * maintain an inventory of managed service providers and evaluate contracts for security considerations |
| **Evaluate cyber protection systems needs** | * implement and configure network defense tools, such as physical and virtual firewalls for servers and endpoints * ensure network infrastructure operating platforms are current * implement a DNS filtering service * evaluate network-based URL filtering based on reputation-based or category-based filters * securely administer remote enterprise hardware and software systems * evaluate segmenting enterprise network and filter for malicious traffic between segments * consider additional email authentication services |

### Detect

Develop and implement appropriate procedures to identify security risks that may impact delivery of critical services.

| **Task** | **Considerations** |
| --- | --- |
| **Develop vulnerability management process** | * establish a risk-based vulnerability remediation strategy * develop plan of action and implement compensating controls for vulnerabilities that cannot be addressed * implement a risk-based patch/update policy * consider when and how to test patches before deployment * consider enabling automatic updates to operating systems and applications, where possible |
| **Enable malware protection** | * select and configure malware protection on computers and servers * implement a schedule to perform periodic scans * configure automatic updates * disable auto-execute functions for removable media, at the group policy level * consider incorporating Endpoint Detection and Response (EDR) |
| **Establish a log retention and review process** | * confirm appropriate logging is enabled on critical systems * standardize logging time stamps * determine where and how long to retain system logs, and maintain adequate storage * identify the frequency and procedures to review logs, and how to handle unusual activity or unauthorized assets * monitor privileged accounts and their access |

### Respond

Develop and implement appropriate activities to take action on a detected security incident.

|  |  |
| --- | --- |
| **Task** | **Considerations** |
| **Develop incident response plan** | * establish and maintain an incident response plan for responding to a security incident * identify an incident response manager and maintain a stakeholder contact list * train staff on use of the incident response plan |
| **Test incident response plan** | * test, conduct exercises on, and update the operation of the plan periodically to ensure it is appropriate and functional * conduct monthly tabletop exercises |
| **Establish relationships with response partners** | * onboard into the DIR Managed Security Services Program * develop pre-incident connections with local, state, and federal law enforcement organizations |

### 

### Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

| **Task** | **Considerations** |
| --- | --- |
| **Develop disaster recovery and business continuity plan** | * establish and maintain a disaster recovery plan for recovering data and applications in the event of loss or damage * identify the conditions for when a security incident necessitates disaster recovery plan activation * train staff on use of the disaster recovery plan * test the disaster recovery plan and solution |

### Supporting Long-term Success

These tasks may help support long-term success of a cybersecurity program, to improve maturity and maintain the program’s operations over time.

|  |  |
| --- | --- |
| **Task** | **Considerations** |
| **Establish an after-action report process** | * after an incident, conduct a hot wash and/or after-action review session with relevant stakeholders * develop an after-action report and associated corrective action plan to assign follow-up activities to the appropriate stakeholder |
| **Consider conducting post-incident assessments** | * after incident recovery, consider performing a security assessment to verify recovery activities and produce an updated gap analysis * consider performing a penetration test to verify recovery configurations |
| **Evaluate public information protections for security information** | * evaluate Texas Government Code section 552.139 as it relates to protecting sensitive information from release |
| **Engage with your community** | * take part in community information sharing or coordination * consider joining the Texas ISAO * find a regional cybersecurity working group |

## Supporting Resources

These supporting resources are available free or at a reduced cost to support security program development.

| **Phase** | **Resource** |
| --- | --- |
| **Set-Up** | Multi-State Information Sharing and Analysis Center (MS-ISAC) and the CIS Security Best Practice Team’s [First Steps Within a Cybersecurity Program](https://www.cisecurity.org/wp-content/uploads/2021/03/MS-ISAC-First-Steps-Within-a-Cybersecurity-Program.pdf) |
| Texas [Cybersecurity Awareness Month Resources](https://dir.texas.gov/information-security/cybersecurity-awareness-month) |
| **Identify** | Texas DIR [Managed Security Services (MSS)](https://dir.texas.gov/shared-technology-services/managed-security-services)- Risk and Compliance Services |
| [Texas Cybersecurity Framework](https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Framework%20Controls%20and%20Definitions.pdf) |
| Cybersecurity and Infrastructure Security Agency (CISA) [Cybersecurity Assessments and Technical Services](https://us-cert.cisa.gov/resources/ncats) |
| Cybersecurity and Infrastructure Security Agency (CISA) [Cybersecurity Assessments and Technical Services](https://us-cert.cisa.gov/resources/ncats) – Cyber Hygiene: Vulnerability Scanning |
| CISA Insights [Risk Considerations for Managed Service Provider Customers](https://www.cisa.gov/sites/default/files/publications/cisa-insights_risk-considerations-for-msp-customers_508.pdf) |
| Department of Homeland Security/MS-ISAC [Nationwide Cybersecurity Review](https://www.cisecurity.org/ms-isac/services/ncsr/) |
| Center for Internet Security (CIS) [Policy Template Guide](https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf) and [CIS Controls](https://www.cisecurity.org/controls/cis-controls-list/) |
| CIS [Controls V8](https://www.cisecurity.org/controls/v8/) |
| Conference of State Bank Supervisors [Ransomware Self-Assessment Tool](https://www.csbs.org/ransomware-self-assessment-tool) |
| **Protect** | Texas DIR [Managed Security Services (MSS)](https://dir.texas.gov/shared-technology-services/managed-security-services) - Security Monitoring and Device Management Services (SMDM) |
| Texas DIR [Statewide Cybersecurity Awareness Training Resources](https://dir.texas.gov/information-security/statewide-cybersecurity-awareness-training) |
| CISA and MS-ISAC Joint Ransomware Guide [Part 1: Ransomware Prevention Best Practices](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf) |
| Multi-State Information Sharing and Analysis Center (MS-ISAC) [Malicious Domain Blocking and Reporting (MDBR) Service](https://www.cisecurity.org/ms-isac/services/mdbr/) and other MS-ISAC [Cybersecurity Services](https://www.cisecurity.org/services/cis-cybermarket/training/sans-online-technical-training/) |
| Center for Internet Security Cyber Market [SANS Online Technical Training](https://www.cisecurity.org/services/cis-cybermarket/training/sans-online-technical-training/) |
| Federal Virtual Training Environment (FedVTE) [Free Online Cybersecurity Training](https://fedvte.usalearning.gov/) |
| **Detect** | Texas DIR [Managed Security Services (MSS)](https://dir.texas.gov/shared-technology-services/managed-security-services) - SMDM |
| Cybersecurity and Infrastructure Security Agency (CISA) [Cybersecurity Assessments and Technical Services](https://us-cert.cisa.gov/resources/ncats) – Cyber Hygiene: Vulnerability Scanning |
| **Respond** | Texas DIR [Managed Security Services (MSS)](https://dir.texas.gov/shared-technology-services/managed-security-services) - Incident Response Services |
| CISA [Cybersecurity Tabletop Exercise Packages](https://www.cisa.gov/publication/cybersecurity-scenarios) |
| CISA and MS-ISAC Joint Ransomware Guide [Part 2: Ransomware Response Checklist](https://www.cisa.gov/stopransomware/ransomware-guide) |
| MS-ISAC [Incident Response Resources](https://www.cisecurity.org/isac/report-an-incident/) |
| American Public Power Association [Public Power Cyber Incident Response Playbook](https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf) |
| **Recover** | Texas DIR Incident Response Team Redbook: Services Restoration Priority Worksheet |
| **Support** | Texas DIR Incident Response Team Redbook: Post-Incident After Action Review and Improvement Plan |
| Cybersecurity and Infrastructure Security Agency (CISA) – [Assessments: Cyber Resilience Review (CRR)](https://us-cert.cisa.gov/resources/assessments) |

# 

# Appendix C: Glossary and Acronyms

## Glossary

The table below identifies terms and definitions relevant to cybersecurity.

| Term | Definition |
| --- | --- |
| Admissible Evidence | Evidence that is accepted as legitimate in a court of law, *see* Chain of Custody. |
| 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. |
| Authorized User | A person granted certain permissions to access, manage, or make decisions regarding an information system or the data stored within the system. |
| Authorized Use and Disclosure | A permissible action or use of confidential information. |
| Authorization | The act of granting a person or other entity permission to use data or computer resources in a secured environment. |
| Availability | The security objective of ensuring timely and reliable access to and use of information. |
| Breach | An impermissible 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 | Applicable to 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 Sensitive Personal Information. Breached SPI that is also Protected Health Information (PHI) may also be a HIPAA breach, to the extent applicable. |
| Breach of PHI (HIPPA Definition) | With respect to PHI pursuant to HIPAA Privacy and Breach Notification Regulations and regulatory guidance any unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations is presumed to be a breach unless a covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Compromise will be determined by a documented risk assessment including at least the following factors:   * The nature and extent of the confidential information involved, including the types of identifiers and the likelihood of re-identification of PHI. * The unauthorized person who used or to whom PHI was disclosed. * Whether the confidential information was actually acquired or viewed. * The extent to which the risk to PHI has been mitigated. |
| With respect to PHI, a “breach” pursuant to HIPAA Breach Regulations and regulatory guidance *excludes*:   * Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations. * Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business Associate location to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement as defined by HIPAA in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations   A disclosure of PHI where a covered entity or business associate demonstrates a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, pursuant to HIPAA Breach Regulations and regulatory guidance. |
| Business Continuity Plan | The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption. |
| Chain of Custody | Refers to the application of the legal rules of evidence and its handling. |
| Confidential Information | Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. This includes any communication or record (whether oral, written, electronically stored, or transmitted, or in any other form) that consists of or includes any or all of the following:   * Federal Tax Information sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the organization. * Personal Identifying Information. * Sensitive Personal Information. * Protected Health Information, whether electronic, paper, secure, or unsecure. * Social Security Administration data sourced from the Social Security Administration under a data sharing agreement with the organization. * All non-public budget, expense, payment, and other financial information. * All privileged work product. * Information made confidential by administrative or judicial proceedings. * All information designated as confidential under the laws of the State of Texas and of the United States, or by agreement.   Information identified in a contract or data use agreement to which 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. |
| Contingency Management Plan | A set of formally approved, detailed plans and procedures specifying the actions to be taken if or when circumstances arise. Such plans should include all eventualities ranging from key staff absence, data corruption, loss of communications, virus infection, partial loss of system availability, etc. |
| Data | Information in an oral, written, or electronic format that allows it to be retrieved or transmitted. |
| 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. |
| Hardware | The physical technology used to process, manage, store, transmit, receive, or deliver information. The term does not include software. Examples include laptops, desktops, tablets, smartphones, flash drives, mobile storage devices, CD-ROMs, and access control devices. |
| Harm | Although relative, the extent to which a privacy or security incident may cause damage to an organization or harm to an individual, reputation, financial harm, or results in medical identity theft. |
| Incident | An event which results in the successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system. |
| Incident Response Lead | The person who is responsible for the overall information security incident management within an organization and is responsible for coordinating the organization’s resources, to prevent, prepare, respond, or recovery 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 and security staff that aids in protecting the privacy and security of information that is confidential by law and provides a central resource for an immediate, effective, and orderly response to Incidents at all levels of escalation. |
| Information Security | The administrative, physical, and technical protection and safeguarding of data (and the individual elements that comprise the data). |
| Integrity | The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. |
| Local Area Network (LAN) | A private communications network owned and operated by a single organization within one location. |
| Malicious Code | A software program that appears to perform a useful or desirable function but gains unauthorized access to computer system resources or deceives a user into executing other malicious logic. |
| Malware | A generic term for different types of malicious code. |
| Penetration | Gaining unauthorized logical access to sensitive data by circumventing a system’s protections. |
| Protected Health Information (PHI) | Information subject to HIPAA. Individually identifiable health information in any form that is created or received by a HIPAA Covered Entity, and relates to the individual’s healthcare condition, provision of healthcare, or payment for the provision of healthcare as further described and defined in the HIPAA Privacy Regulations. PHI includes:   * Demographic information unless such information is De-identified as defined in the HIPAA Privacy Regulations. * “Electronic Protected Health Information” and unsecure PHI as defined in the HIPAA Privacy Regulations. * The PHI of a deceased individual within 50 years of the date of death. * Employment information. |
| Personal Identifying Information (PII) | As defined by the Texas Business and Commerce Code Section 521.002(a)(1), “personal identifying 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 recreating files which have disappeared or become corrupted from backup copies. |
| 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. The process includes identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls. |
| Sensitive Data | While not necessarily protected by law from use or disclosure, data that is deemed to require some level of protection as determined by an individual organization’s standards and risk management decisions. Some examples of “sensitive data” include but are not limited to:   * Operational information. * Personnel records. * Information security procedures. * Internal communications. * Information determined to be authorized for use or disclosure only on a “need-to-know” basis. |
| Sensitive Personal Information (SPI) | As defined by the Business and Commerce Code section 521.002(a)(2), SPI means:  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:   * 1. Social security number.   2. Driver’s license number or government-issued identification number.   3. 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.  1. Information that identifies an individual and relates to:    1. The physical or mental health or condition of the individual.    2. The provision of health care to the individual.    3. 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. |
| Server | A processor computer that supplies a network of less powerful machines (such as desktop PCs and laptop computers) with applications, data, messaging, communication, information, etc. |
| Threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals. |
| Traffic Light Protocol | The Traffic Light Protocol (TLP) facilitates easier sharing of information. TLP is a set of “classifications” used to describe with whom sensitive information can be shared. TLP only has four designations:   * TLP:RED - Not for disclosure, restricted to participants only. * TLP:AMBER - Limited disclosure, restricted to participants’ organizations. * TLP:GREEN - Limited disclosure, restricted to the community. * TLP:WHITE - Disclosure is not limited. |
| Vulnerability | A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. |
| Wide Area Network (WAN) | A communications network that extends beyond the organization’s immediate premises. |

## Common Acronyms

The table below provides a list of acronyms and descriptions common 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 Act | Health Information Technology for Economic and Clinical Health Act (2009) |
| IRS | Internal Revenue Service |
| IRT | Incident Response Team |
| ISO | Information Security Office |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PHI | Personal Health Information |
| PIA | Public Information Act, Texas Gov’t Code Ch. 552 |
| PII | Personal Identifying Information |
| SPI | Sensitive Personal Information |
| SSA | Social Security Administration |
| TAC | Texas Administrative Code |
| TLP | Traffic Light Protocol |



1. Verizon 2021 Data Breach Investigations Report [↑](#footnote-ref-2)