i

Travis County

Technology and Operations Information Security Incident Response Plan

Version 2.8

July 2023

For questions or further information, please contact:

	Name	Phone	Email
Sponsor	Brandon Rogers (CISO)	512-854-1222	Brandon.Rogers@traviscountytx.gov
Owner	Melissa Ojeda (Technology Operations and Security-Disaster Recovery)	512-854-1838	Melissa.Ojeda@traviscountytx.gov

"Sponsor" is the executive responsible for compliance
"Owner" is the owner of this document

APPROVAL SIGNATURES

This plan, as prepared by Travis County Technology and Operations Information Security describes the Incident Response Plan for all information systems managed by the Chief Information Officer (CIO) and Commissioners Court as outlined in Travis County Code, Chapter 35. The Travis County Security Incident Response Team (TCSIR -Team), under the guidance of the CIO, is authorized to take appropriate steps deemed necessary to contain, mitigate, and/or resolve information security incidents. The TCSIR-Team is responsible for investigating suspected security incidents and reporting findings to management and the appropriate authorities as necessary.

This plan is hereby submitted to the proper security authority for review and approval.

Approved By: Approved by Brandon Rogers 10/25/2021
[Brandon Rogers] Date
[Chief Information Security Officer]

Program Maintenance

Frequency	Action
Annually	Review, update, and distribute the Security Incident Response Plan as needed.
Annually	a. Test the plan via a checklist, procedure verification, or walk-through analysis. b. Document lessons learned c. Update and distribute the plan, if needed.

Version History

Date Revised	Version	Revision Description
8/20/2015	1.0	Initial Plan Creation
3/24/2016	1.1	Added notification of CJIS, HIPAA and PCI Compliance Officers to 2.2, 2.4, 2.8, 3.2.3, 3.4, 4.2
4/12/2016	1.2	Administrative Technology and Operations for grammar and formatting. No substantive changes.
6/27/2016	1.3	Described responsible party in 2.7. Clarified notification parameter in 2.8. Basis for public engagement in Security Incident added to 3.2.3. Modified 4.2 step 2 to allow for circumstances when a witness might not be interviewed.
3/5/2018	1.4	Updated title to "Information Security." Updated Severity Level, Response Level and Security Incident Threat Matrix tables. Updated Security Incident Response Resources section. Condensed Approval Signature Section. Updated to reflect new Chief Information Officer. Added Appendices A, B, C, D, E and F.
5/23/2019	1.5	Added Election Information to 2.3, 2.4, and 3.3. Changed appropriate Technology and Operations Information Security team member to TC technology resource in 3.3.
10/01/19	1.6	• Updated from May 2019 version. Revised Incident Response Plan from older version
12/26/19	1.7	Added and revised multiple sections
2/19/20	1.8	Updates to the following: • Overview • Roles and responsibilities Threat matrix sections
2/27/20	1.9	Updates to Incident Response Process

3/2/20	2.0	Updates to contacts in Information and Technology Security Contacts
11/13/2020	2.1	Updates: 1. Paul K. updates
4/16/2021	2.2	Updates: 1. Updates to table of contents, page numbers, contact information
7/21/2021	2.3	Updates: 1. Personnel titles updated
10/21/2021	2.4	Updated language throughout document, corrected fonts in Section 3
1/21/2022	2.5	1. Added section 7: OAG data 2. Updated Contact Information
5/2/2023	2.6	1. Updated contact Information
6/29/2023	2.7	1. Updated language throughout document
7/24/2023	2.8	1. Added members to the notification list in section 4.2

Contents

Table of Contents

Incident Response Policy

Travis County Security Incident Response Policy

Policy #: TC-Technology and Operations Information Security-125
Approved By: Paul Hopingardner, Chief Information Officer
Version #: 1.3 **Effective Date**: May 30, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Travis County, and document security incidents and their outcomes.

Policy

Travis County will do the following:

- Identify, research, and respond to any suspected security incidents in a timely manner
- Mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents
- Maintain appropriate documentation for all security incidents

Procedure(s)

Travis County will maintain procedures for identifying events that qualify as security incidents. A security incident is any breach of security policy or any activity that could potentially put sensitive information at risk of unauthorized use, disclosure, or modification.

A breach, such as one as defined under the HITECH Act or Texas Breach Law, or CJIS, may have occurred if the incident involved ePHI, PII, CJI or other sensitive information. A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information (as defined below), which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, members of the workforce must immediately follow the instructions in TC-Technology and Operations Information Security-501, Data Breach Discovery Policy.

Incidents will be classified by the following severity level:

- **RED:** High risk of financial, data, and reputation loss as well as downtime (Regulatory Data or Financial Fraud involved).
- **YELLOW:** Small risk of financial, data, or reputation loss. Some downtime may be experienced. (No Regulatory Data or Financial Fraud involved).
- **GREEN:** Potential interruption of normal daily operations. Minimal financial, data, and reputation loss risks. Security concern that needs to be addressed.

Response level dictates how quickly the response needs to be and who should be activated to respond

- **Level 1**: These are the most severe security incidents facing Travis County. All the Travis County Security Incident Response Team TCSIR-Team will be involved in the immediate response effort. A FORMAL INCIDENT REPORT IS REQUIRED.
- **Level 2**: These are not as severe as Response Effort 1 but are still very serious. The response by the majority of the TCSIR-Team needs to be quick, if not immediate. A FORMAL INCIDENT REPORT IS REQUIRED.
- **Level 3**: These security incidents have some impact on the infrastructure, but do not pose a large threat for Travis County. A small number of TCSIR-Team members will be involved in handling

Severity 4 security incidents. NO FORMAL INCIDENT REPORT IS REQUIRED

- **Level 4**: Security incidents that will need to be investigated. NO FORMAL INCIDENT REPORT IS REQUIRED.

Please see the Travis County Incident Response Plan "Incident Threat Matrix" for determining Severity and Response Level.

All workforce members of Travis County will report any security incident to their department or office management team and to the Technology and Operations Information Security Service Desk. If ePHI or PII is involved, also notify the HIPAA Privacy Officer, HIPAA Security Officer, and the CIO, or their designee, that they become aware of or suspect, as soon as practical. If CJI is involved, notify the Travis County CJIS Local Agency Security Officer (LASO).

Workforce members will not disclose the incident information to anyone other than the Chief Information Officer or their designee, HIPAA Security Officer, HIPAA Privacy Officer, LASO, and their department or office management team, and will not disclose any information about the incident to anyone or in any place outside of Travis County.

Workforce members must report security violations as quickly as possible after discovery to their immediate supervisors, the Technology and Operations Information Security Service Desk Information Security group, or designees, as appropriate. If the violation involves protected health information, workforce members must also report to the HIPAA Privacy Officer and the HIPAA Security Officer, CJIS LASO or designees, as appropriate, depending on the type of information involved.

Travis County will maintain procedures for responding to serious and non-serious security incidents to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Incidents characterized as Level Red or Yellow Severity the CIO, HIPAA Privacy Officer and HIPAA Security Officer, LASO and/or the department or office management team or their designee, will be responded to immediately.

Travis County will attempt to mitigate any harmful effects, when possible, of security.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Randy Lott	05/30/2015
1.1	Modified procedure to include event terminology.	Security Policy Team	01/15/2016
1.2	Merged Response and Reporting Policy (119) into this policy.	Security Policy	08/19/2016
1.3	Consolidated Severity Levels to RED, YELLOW and GREEN. Consolidated Response Levels to 1, 2, 3 and 4. Updated name due to new CIO.	Randy Lott	03/19/2018

Introduction

Overview

Security Incident Response is defined as an organized approach to addressing and managing the aftereffects of a security breach or attack (also known as a security incident). The goal of a security incident response program is to handle the situation in a way that limits Technology and Operations damage and reduces recovery time and costs. The following document describes the Travis County Security Incident Response Plan for handling real and perceived security incidents to limit damage and to respond accordingly.

Purpose

The purpose of this Security Incident Response Plan is to provide general guidelines on responding to security incidents effectively and efficiently by identifying, containing, mitigating, and reporting security incidents. This document guides agency response to information security incidents in accordance with federal and state rules and regulations, to include those defined in the HIPAA privacy and security standards; the Payment Card Industry data security standard (PCI DSS); and the Criminal Justice Information Services Security Policy (CJIS). These initiatives are critical to identify, document, and protect the organization against unauthorized activity to sensitive information belonging to customers, employees, contractors, third parties, and the County at-large.

Scope

This Security Incident Response Plan applies to employees, contractors, consultants, temporary employees, and other staff members at Travis County, including all personnel affiliated with third parties conducting business on and off Travis County premises. This Plan applies to all physical and virtual equipment that is owned or leased by Travis County.

Technology and Operations Information Security Incident Response Resources

This plan is designed to be a resource reference while responding to a security incident. Other resources may be necessary to completely investigate and document a security incident, examples of which follow:

- Security Incident Response Plan
- Contact information for ISP, MSSP, AV/Malware Vendor, other 3rd party security services
- Contact information for local/state/federal law enforcement
- Current Network Diagrams
- Current Information Asset Inventory
- Disaster Response and Business Continuity Plans
- Technology and Operations On-Call/Roster information
- Compliance or regulatory bodies required reporting
- Standard Operating Procedures/ Runbooks for specific types of attacks
- General application documentation
- Policies, procedures, and standards promulgated by independently elected and appointed officials
- Current Travis County Org Chart

Definition of a Security Incident

Travis County defines a security incident as an event that actually or potentially results in adverse consequences to a Travis County information system or data that the system process, stores, or transmits. Security incidents that qualify as needing the attention of the TCSIR-Team, may include, but are not limited to the following:

- Theft or loss of a Travis County computing asset
- Vulnerability exploited in an information system
- Outbreak of malicious software
- Denial of Service (DoS) attack / Distributed Denial of Service (DDoS) attack
- Unauthorized entry in Travis County applications or network
- Data Breaches for HIPAA, CJIS, Election Information, PCI or PII.
- Phish, Spear Phish, Whaling resulting in the loss of credentials
- Ransomware
- Business Email Compromise
- Authorized investigation of an insider threat

SECTION 1 Glossary, Acronyms and Responsibilities

1.1 Glossary

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 of **Confidential Information** such that the use or disclosure poses a significant risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Depending upon applicable law, "Breach" may for example mean:

1) HIPAA Breach of Protected Health Information ("PHI"). 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:
    a. The nature and extent of the **Confidential Information** involved, including the types of identifiers and the likelihood of re-identification of PHI.
    b. The unauthorized person who used or to whom PHI was disclosed.
    c. Whether the Confidential Information was acquired or viewed; and
    d. 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*:
    a. 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.
    b. 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 arrangements

defined by HIPAA in which the Covered Entity participates, and the information received because of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations

c. 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.

2) Breach in Texas. Breach means "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 Ch. 521, that compromises the security, confidentiality, or integrity of Sensitive Personal Information. Breached SPI that is also PHI may also be a HIPAA breach, to the extent applicable.
3) Any unauthorized disclosure as defined by any other law and any regulations adopted thereunder regarding **Confidential Information**.

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 Technology Operations and Security 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:

1) Federal Tax Information sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the agency.
2) Personal Identifying Information.
3) Sensitive Personal Information.
4) Protected Health Information, whether electronic, paper, secure, or unsecure.
5) Social Security Administration data sourced from the Social Security Administration under a data sharing agreement with the agency.
6) All non-public budget, expense, payment, and other financial information.
7) All privileged work product.
8) Information made confidential by administrative or judicial proceedings.
9) All information designated as confidential under the laws of the State of Texas and of the United States, or by agreement; and
10) Information identified in a contract or data use agreement to which an agency 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 agency contractor, including events reported by a third party to an agency or agency 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, thumb 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 agency 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: person responsible for the overall information security Incident management within an agency and is responsible for coordinating the agency's resources which are utilized in the prevention of, preparation for, response to, or recovery from any Incident or Event.

Incident Response Team (IRT): led by the Incident Response Lead, the core team composed of subject- matter experts and 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.

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; and
- employment information.

Personal Identifying Information (PII): as defined by the Texas Business and Commerce Code §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; and
- telecommunication access device as defined by the Penal Code §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: process of recreating files which have disappeared or become corrupted from backup copies.

Regulated 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 agency.
- Personal Identifying Information.
- Sensitive Personal Information.
- Protected Health Information, whether electronic, paper, secure, or unsecured.
- Social Security Administration data sourced from the Social Security Administration under a data sharing agreement with the agency.
- 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; and
- Information identified in a contract or data use agreement to which an agency contractor specifically seeks to obtain access for an Authorized Purpose that has not been made public.

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 of 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.

Security Incident- Travis County defines a security incident as an event that actually or potentially results in adverse consequences to an information system or data that the system processes, stores or transmission. Security incidents that qualify as needing the attention of the TCSIRT, may include, but are not limited to the following:

- Theft or loss of a Travis County computing asset
- Vulnerability exploited in an information system
- Outbreak of malicious software
- Denial of Service (DoS) attack / Distributed Denial of Service (DDoS) attack
- Unauthorized entry in Travis County applications or network
- Data Breaches
- Phish, Spear Phish, Whaling resulting in the loss of credentials
- Ransomware
- Authorized investigation of an insider threat (bad actor)

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 agency's standards and rise 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 Texas Business and Commerce Code

§521.002(a)(2) means:

1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and items are not encrypted:
    a. Social security number.
    b. Driver's license number or government-issued identification number; or
    c. 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; or
2) Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual.
    b. The provision of health care to the individual; or
    c. Payment for the provision of health care to the individual.

The term "Sensitive Personal Information" 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.

Vulnerability: 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 organizations immediate premises.

1.2 Common Acronyms

CFAA: Computer Fraud and Abuse Act (1986)
CIO: Chief Information Officer
CISO: Chief Information Security Officer
CJIS: Criminal Justice Information Services, a division of FBI
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
NIST: National Institute of Standards and Technology
PHI: Personal Health Information
PIA: Public Information Act, Government Code Ch. 552
PII: Personal Identifying Information
SPI: Sensitive Personal Information

TAC: Texas Administrative Code

1.3 Roles and Responsibilities

Travis County Security Incident Response Team (TCSIR-Team) is established where the Travis County Information Technology Services (Technology and Operations) Department is the coordinated entity. The Security Incident Response Coordinator (SIRC) and the Technology and Operations Incident Response Manager will be assigned by the CIO and will serve as the primary points of contact (POC) through the life of security incident response efforts. This type of structure will ensure the security incident response process is developed and information sharing is facilitated.

Additional response team members can be assembled from other departments, if applicable, to a response that will coordinate and report back to the Technology and Operations Department.

Security incident response is contained primarily in-house for Travis County; however, provisions may be in place to partially outsource response support as necessary. Travis County may utilize Incident Response (IR) services provided by 3rd. party security providers as part of their team structure and response capabilities.

The TCSIR-Team core group responsible for responding to network or computer related security incidents is made up of members from the technology and operations Security, Applications, Operations and Networking teams, 3rd party security providers, other Travis County Departments, and other elected and appointed official technical staff, as required.

Role	Responsibility
Technology and Operations	
Chief Information County Executive	The Chief Information County Executive provides support, as needed, to keep response moving forward, informs the Technology Operations Security of possible incidents, ensures resources are available to help in the incident recovery efforts and information gathering, and makes business-related decisions based on input from members of the team.
Director of IT	Director of IT ensures resources are available to help with incident response and recovery efforts. Supports all ITS teams in response and recovery.
Network Team	Network Administrators provide knowledge and expertise in their specific field related to an incident. They will also help with any remediation within their field.
Help Desk	The helpdesk will receive possible incident reports and help with information gathering. They will also be helping with any remediation within their field.
System Owner	Responsible for providing necessary access to operating system and data contained within systems they own.
Technology and Operations Information Security	

Chief Information Security Officer (CISO)	*The CISO* is responsible for overseeing incident investigations in coordination with the Incident Response Team [1 TAC §202.26]. This includes: • Establishing and documenting incident response procedures, standards, and guidelines [1 TAC §202.21] • Making recommendations for TSIRT members [1 TAC § 202.26]; • Identifying, containing, mitigating, and reporting privacy or security incidents that involve propagation to external systems, violation of applicable federal and state laws which requires involvement from law enforcement, or potential modification or disclosure of confidential information. • Assigning incident severity level. • Determining the physical and electronic evidence to be gathered as part of the incident investigation.

	• Communicating with appropriate parties regarding the security incident during and after the investigation; and • Preparing the incident report to include recommendations based on lessons learned.
Privacy Officer (PO)	The Privacy Officer documents the types of personal information that may have been breached; provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information; assists in developing appropriate communication to impacted parties; and assesses the need to change privacy policies, procedures, and/or practices as a result of the incident.
PCI Compliance Person	Responsible for reporting any security incidents that involves credit card information.
CJIS LASO	Responsible for policies and procedures regarding specific types of sensitive data. The CJIS LASO (Local Agency Security Officer) will be the TCSO point of contact for any security incident that requires Technology Operations and Security to notify law enforcement.
Travis County Information Security Incident Response Team {TCSIRT)	Incident Response Team members are employees of Travis County Technology and Operations Information Security as well as outside contractors who gather, preserve, and analyze evidence so that an incident can be investigated and concluded.
Security Incident Response Coordinator (SIRC) (Security Architect)	The SIRC will maintain this Security Incident Response Plan, Security Incident Reports, and records. They are also responsible for coordinating and documenting all Security Incident Response Plan (SIRP) tests and any required training.
TECHNOLOGY AND OPERATIONS Business Continuity/Disaster Recovery	Responsible for assessing the impact of a security incident on IT business processes and updating necessary documents. Business continuity planners offer expertise in minimizing operational disruptions.
Security Operations Teams	Responsible for managing and monitoring the security tools for Travis County Technology and Operations systems. Also responsible for security incident remediation
Information Assurance	Responsible for reviewing security policies
Human Resources	
Director of Human Resources	If an incident involves a current or former employee, contractor, or business partner, the Director of Human Resources will be notified to evaluate the incident from a personnel perspective.
Communications and Records Services (CARS)	Responsible for communications between the agency and the public during and after an incident.
Public Information Office	Public Information Office is the liaison between the Travis County and the public during and after an incident.
Commissioner's Court	
County Attorney and Attorneys	County Attorney provides counsel on the extent and form of all disclosures to law enforcement and the public and provides advice regarding liability issues in the event an incident affects patients, customers, employees, or the public
Law Enforcement	includes federal and state law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information. The County Attorney will coordinate interactions with law enforcement
County Judge	The County Judge provides support, as needed, to keep response moving forward. Responsible for final decisions and approvals.

SECTION 2 Technology and Operations Security Incident Process

2.0 Technology and Operations Information Security Incident Response Process

The Security Incident Response Planning process (described above) provides fundamental information needed for the operation and execution of the SIRP. Upon completion of the Security Incident Response Process, data is fed into the Post Incident Process to identify areas where the SIRP was not operating as intended. This continuous process improvement method ensures the SIRP is developed and updated to meet the needs of the organization.

2.1 Incident Identification

The Identification phase is the trigger for initiating the Security Incident Response Process. Anyone can identify a security incident; however, there are several key steps that must be executed to ensure the security incident does not cause further damage to the organization.

a. Travis County Technology and Operations Information Security Service Desk: For all real or perceived security incidents, the person who has identified the event must contact the Travis County Technology Operations and Service Desk. Each Service Desk employee has contact information to escalate an event if it is deemed necessary. A Security Incident Report (IR) shall be opened within the Technology and Operations Information Security ticketing system.

b. Incident Handling Form- Start documenting information on the event and impacts. Refer to Incident Handling Form in **Appendix I.**

2.2 Response to Initial Notification

The following table describes the relationship between the person who identified the security incident and the handoff to a Security Incident Response Team:

Stage	Who	Does What
1	• Systems Engineers or Application Developers • Affected End User • Affected System owner (Dept/Office) • External Business Partner/Third Party • Technology and Operations Service Desk • Technology and Operations Information Security Analyst	Makes the initial notification of an event. Work with appropriate Technology and Operations staff to determine nature of the event. If it is determined that this is an information security incident, the Technology and Operations Security Operations Team is informed.
	Information Security Operations, along with other Technology and Operations assets	Determine Response Level (1. 2. 3 or 4). Notify CISO, Technology and Operations and other appropriate Travis County personnel of the security incident, depending up on Technology and Operations Response Level and scope.

2.3 Internal Notification Procedures

Security Operations should use the following table as a guide to determine whom to contact regarding a security incident. A variety of personnel could be notified based on the security incident type and Security Incident Severity category.

Security Operations should use the following table as a guide to determine whom to contact regarding a security incident

When	Contact
A security incident impacts specific operating systems, infrastructure components or unauthorized wireless access points	Ad-hoc security incident response team members (platform specific engineers, database administrators, network engineers, etc.)
A security incident cannot be resolved without impacting the business operations; or involves a service provider or contracted 3rd party. Containment or eradication solution may impact business operations were County revenue could be lost, or customer service impacted.	CISO, or designee, will coordinate with the County Attorney's Office, the affected department or elected official, Commissioners Court, the affected Business/System Owner, or sponsor of the contracted entity.
A security incident that involves a Travis County employee	CISO, or designee, may coordinate with the affected department management or independently elected official and their management team, as is appropriate.
A security incident involving the theft or destruction of an information system and could be criminal in nature	CISO, or designee, may coordinate with the County Attorney's Office, the affected department or elected official, Privacy Officer, CJIS LASO and/or PCI Compliance Officer (if designated) and Commissioners' Court. They will decide when/if to communicate to law enforcement.
Sensitive information (to include regulatory information) is vulnerable or may have been breached	CISO, or designee, will coordinate with the County Attorney's Office, the affected department or elected official, Privacy Officer, CJIS LASO and/or PCI Compliance Officer (if designated), Commissioners' Court and the Public Information Officer. They will ensure the organization acts in accordance with Federal and State Breach Notification Laws.
A security incident is large enough that external media may be interested, or Travis County may need to provide "damage control" messages to customers or the public	CISO, or designee, will coordinate with the County Attorney's Office, the affected department or elected official, Privacy Officer, CJIS LASO and/or PCI Compliance Officer (if designated), HRMD Risk Manager, Commissioners' Court and the Public Information Officer who will then decide when/if to engage the public.
An incident where a complete shut-down or destruction of Travis County's central location and/or the Travis County's computer systems (Catastrophic Disaster)	The CISO will contact the County Judge who has the authority to declare a disaster, if believed necessary. At that point, the County and Technology and Operations-specific Disaster Recovery Plans/Continuity of Operations Plans are implemented, and this plan may be used as reference

2.4 Incident Investigation

The goal of the Investigative phase is to gather and analyze information associated with an event to determine the scope a security incident. The intent is to identify activity, which poses a threat to Travis County systems, as well as any deviations from normal day-to-day operations.

The following table (Table 9) describes the steps to follow when conducting the initial Security Incident Investigation for a possible Response Level 1 or 2 Incident:

1	Security Operations and other appropriate TC technology resource	Is it clear that this event is a Response Level 1 or 2 security incident and immediate action is required? Example: a propagating virus, ransomware, business email compromise or lost or stolen mobile device with regulatory data Yes- Proceed to the Security Incident Mitigation and Analysis section and take immediate action. No- Step 2
2		Document information obtained on the event in both Change Gear and the Proofpoint Threat Response Panel.
3		Based on system(s) affected, contact the appropriate security incident response team member(s).
4		Gather all information about the event. This data will reside in the Proofpoint Threat Response Panel. a. Interview the person reporting the security incident. b. Collect the affected system logs along with associated artifacts (event logs, etc.). Collect and preserve all appropriate reporting systems information (firewall, intrusion prevention, anti-virus).
5		Security Incident Reporting Form
6		Based on the analysis of the event, determine the Response Level. If it is a Level 1or 2, proceed to the Security Incident Mitigation and Analysis section (3.4) of this plan and take immediate action. Notify members of the TCSIR-Team. If the Response Level is 3 or 4, Security Operations will document the severity of this security incident and business lines affected in Change Gear and the Proofpoint Threat Response Panel, while also notifying the appropriate parties

2.5 Incident Mitigation and Analysis

The goal of this phase is to respond immediately to the security incident and prevent the security incident from escalating further, as well as gather possible evidence. The response will depend on the nature and extent of the security incident.

Consider these factors when determining the best strategy for mitigating and analyzing a security incident:

- Potential damage to the system
- Potential theft of information resources
- Preservation of evidence
- System or service availability
- Time and resources available to implement the recovery strategies

The TCSIR-Team should use the following table (Table 10) as a guide to determine what the best option is for mitigating the security incident:

IF	CONSIDER
The security incident could potentially spread to other systems or damage critical data or information	Disconnecting the compromised system from the network.
The compromised system must be operational in order to continue business operations or to track activities of the intruder or Travis County has decided to pursue prosecution and law enforcement has asked the organization to allow the activities of the intruder to continue.	Taking alternative containment actions and leave the system running.
The attack tool is deleting data from the system.	A hard shut down of the system (i.e. pull the plug, power off the system).
An unauthorized device, such as a wireless access point, is detected and attached to the internal network.	Notify the Network team. Determine who is responsible for the area and have them remove the device. Verify device has been removed.

1	CIO or their designee	Establish the SCIR and mobilize the TCSIR-Team (appropriate security incident response team members)
2	TCSIR Team	Begin building the appropriate mitigation strategy based on the containment factors
3		Does the mitigation strategy involve disconnecting or shutting down an operational resource? Yes- Work with the affected area department head, elected or appointed official and CISO, or designee, HRMD Risk Manager, Privacy Officer, CJIS LASO and/or PCI Compliance Officer (if designated) to determine the risk to the business. No- Go to step 5
4		If necessary, did the department head or elected/appointed official approve of disconnecting or shutting down the resource? Yes- go to step 5 No- Use a different containment strategy. For example, • Apply a firewall, router filters, or both • Null route particular IP addresses • Apply patches and harden the system
5		Secure critical information before shutting system down if possible. This could include but is not limited to • Capture a forensic image • Conduct a packet capture, etc.
6		Execute the mitigation strategy
7	Security Incident Response Coordinator	Document steps taken in the Security Incident Reporting Form

2.6 Security Incident Cleanup

During the Clean-up phase, identify the root cause of the security incident and then remove anything causing harm to the organization.

The following table is used as a guide to determine what the best option is for cleaning up from the security incident.

IF	CONSIDER
It's possible that the intruder had elevated privileges or installed a back door to the system or application?	Performing a clean install, which includes: • Formatting hard disks • Reinstalling the operating system from original media • Reinstalling applications
A full reinstall isn't possible and you know the exact date and time of the security incident	Restoring the **system** from a known, good backup tape.

The application and operating system were not compromised, missing, or damaged	Restoring the **data** from a known good backup tape.
The compromise was relatively minor	Performing a system update, which includes: • Cleaning the system manually of modified files • Applying the appropriate patches and updates

The following table describes the steps to follow when executing a Security Incident Cleanup

1	TCSIR Team	Determine the root cause of the security incident. (e.g., a virus, back door, Tool Kit)
2		Based on the root cause of the security incident, select, and perform the appropriate cleaning option.
3		Review trust relationships for compromise. (e.g., trusted systems such as those on the same subnet or on the same domain, certificates).
4		Repair any compromised trust relationships.
5		Improve defenses by implementing the appropriate protection techniques. For example: • Apply firewall, router filters, or both • Move the system to a new name or IP address • Null route particular IP addresses • Change DNS names • Apply patches and harden the system.
6		Change all system and user passwords on the compromised system
7	Security Incident Response Coordinator	Document steps taken in the Computer Security Incident Reporting Form

2.7 Security Incident Recovery

Once the source of the security incident has been removed, the Recovery phase can begin. During recovery phase, the goal is to put the impacted systems back into production with a high level of confidence that the system has been restored to a "pre-incident" state and can be reintroduced in a secure manner.

The following table describes the steps to follow when executing a Security Incident Recovery

1	TCSIR Team	Perform a vulnerability scan of the system to ensure it does not contain unexpected vulnerabilities. Apply additional fixes/patches as required.
2		Place the system into a test environment
3		Monitor the systems performance and operation. Have any abnormalities been identified? Yes- Go to Investigation phase No- Go to step 4
4		Place system into production environment.
5		Monitor the systems performance and operation. Have any abnormalities been identified? Yes- Go to investigation phase No- Go to step 6
6		If the security incident was reported by a third-party, contact third party

		and monitor performance to ensure abnormal activity does not occur.
7		Work with the business to test applications on the system for functionality and to ensure they are behaving normally. Have any abnormalities been identified? Yes- Go to investigation phase No- Go to step 8
8		Notify appropriate personnel that the system has been restored and place into production.
9		Continue monitoring of system for possible abnormalities.
10	Security Incident Response Coordinator	Document steps taken in the Computer Security Incident Reporting Form.

SECTION 3 Technology and Operations Information Security Post Incident Process

The Post-Incident Process has several sections to identify opportunities for improvement within the organization. The analysis completed within the Post-Incident Process is meant to understand the security incident and prevent future security incidents from occurring.

3.1 Post Incident Analysis

After a security incident has been resolved, the TCSIR-Team will perform an analysis to validate the root cause of the issue and gain an understanding of methods to implement to prevent the security incident from occurring in the future.

The following table describes the steps to follow when performing a Post-Incident Analysis.

1	TCSIR Team	Review documentation generated during the Security Incident Response Process.
2		Interview the applicable people involved in the Security Incident Response Process, especially the person who identified the security incident unless this action conflicts with investigative policies and procedures defined by applicable relevant regulatory authority.
3		Review and analyze evidence collection, and investigative reports on the system. For example: • Forensic report from a third-party provider • Information from Law Enforcement • Investigative notes taken by TCSIRT • Review vulnerability scan results
4		Review research on the security incident and identify areas of improvement.
5		Review and edit the Computer Security Incident Reporting Form for accuracy and completeness.

3.2 Post Incident Lessons Learned

After the Post-Incident Analysis, the TCSIR-Team will have an expert understanding of the issue, root cause, and methods for preventing the issue in the future. The goal of the Lessons Learned Process is to ensure all the documentation created during the Security Incident Response Process and Post-Incident Analysis are documented and action plans are created to prevent future harm to the organization.

1	TCSIR Team	Conduct a Lessons Learned meeting after resuming production and/or the Post-Incident Analysis is completed for major security incidents or when applicable). Include all affected parties • Have all affected parties review the documentation? • Have all affected parties sign off on the documentation?
2		If the security incident was reported by a third-party, verify receipt of the report and a high-level summary of actions taken.
3		Update this plan and other policies and/or procedures, if needed.
4		Apply any long-term resolutions. • Fix processes, technology, and improve our security incident handling capabilities. • Complete any follow-up actions from the Lessons learned meeting.
5		Create recommended strategic resolutions for management. • Financial Impact Analysis • Staff Needs • Budget Needs
6		Have all affected parties review and signoff on the documentation
7		Determine if the Internal Notification Procedures defined in 3.2.3 were followed. • Determine if internal and public notification responsibilities have been properly fulfilled. • Correct deficiencies and make recommendations for process improvement. • Evaluate the appropriateness and effectiveness any public engagement.
8	Security Incident Response Coordinator	Complete Lessons Learned Report

3.3 Post Incident Measures and Reporting

As part of the Post-Incident Analysis and Lessons Learned, Performance Measures will be taken for each security incident. These performance measures include, but are not limited to:

- Total hours the TCSIR-Team was involved, from security incident notification to security incident conclusion
- Costs incurred because of a security incident
- Downtime resulting from a security incident
- Successful activities of the TCSIR-Team during a security incident
- Weaknesses identified in resources, training, and/or processes during security incident response

These performance measures will be reviewed annually along with the Security incident Response Plan. Reviewing performance measures of security incidents will assist with internal and external network infrastructure policy reviews, as well as budgetary matters involving additional tools, resources, and staffing levels needed by the TCSIR-Team.

After the Post-Incident Analysis, the Security Incident Response Coordinator will collect all documents created during the security incident and provide a Post-Incident Report to the CISO and other departments, as directed by the CISO. All documentation must be kept and stored in accordance with the organization's retention requirements and legal/regulatory requirements. The documents must be secure from unauthorized access, alteration, and destruction.

SECTION 4 Event Threat, Impact Analysis, and Escalation Criteria

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

4.1 Event Threat and Impact Analysis

Information Security incident response will be managed based on the functional impact of the incident, informational impact of the incident, and recoverability from the incident. The level of severity is a measure of Technology and Operations Information Security impact on or threat to the operation or integrity of the Travis County Technology Operations and Security information and systems. The impact and severity determine the priority for handling the incident, who manages the incident, and the timing and extent of the response.

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.

The Severity Level of a security incident indicates how much risk exposure there is to Travis County. These severity levels can affect Travis County reputation, financial standing, data loss, and agency downtime. The following table (Table 4) describes the severity level according to the colors seen in the below Security Incident Response Threat Matrix.

Severity Level	Description
Red	High risk of financial, data, and reputation loss as well as downtime (Regulatory Data or Financial Fraud involved).
Yellow	Small risk of financial, data, and reputation loss. Some downtime may be experienced. (No Regulatory Data or Financial Fraud involved).
Green	Potential interruption of normal daily operations. Minimal financial, data, and reputation loss risks. Security concern that needs to be addressed.

Response Level

The response level dictates how quickly the TCSIR-Team needs to respond as well as whom on the team needs to be activated. Efforts may require involvement from specific members that make up the core TCSIR-Team. The response effort levels are defined in the table (Table 5) below.

Category	Definition
Extreme Response Level 1	• Threat of loss of life • Compromised ePHI, PCI, CJI, Election Information, PII or credentials • Compromised credentials used to modify environment • Ransomware infection of multiple departments; encrypting local or network storage • Travis County Regulatory Data Infiltrated • Denial of Service (DoS) Distributed Denial of Service (DDOS) **Response Time**: Immediate

	Contact: CISO, PO, County Attorney, Commissioners' Court A post-incident report is required. Certain aspects of the report may be determined to be confidential under Texas Government Code Section 552.139 and excepted from the requirements of Texas Government Code, Section 552.021 (Public Information Act) if it contains information related to the following: • Computer network security (passwords, PIN numbers, access codes, encryption); • The design, operation, or defense of a computer network. • Data collected, assembled, or maintained by or for the agency to prevent, detect, Investigate criminal activity, or network to criminal activity.
High Response Level 2	• Threatens to have a significant impact on most or all Travis County systems or many users. • Poses a potential financial risk or legal liability to the Travis County. • Threatens PHI, PII, SPI, or other confidential data. • Adversely impacts systems or services critical to the operation of the Travis County. • Poses a significant and immediate threat to human safety; or • Has a high probability of spreading to other systems and causing significant damage or disruption? • Targeted campaign directed at specific employees or departments to compromise sensitive business information such as financial records • Stolen or lost laptop or mobile device from department with PII, PCI, CJIS, ePHI data or sensitive financial information • Ransomware infection of single department; encrypting local or network storage • Trojan Virus actively being used as a backdoor into the network or Command and Control (C2, CnC) found and being used **Response Time:** Immediate **Contact:** CISO, PO, County Attorney A post-incident report is required. See the previous reference to the confidentiality of the report according to Texas Government Code section 552.139.
Medium Response Level 3	• Adversely impacts a moderate number of systems, services, and users. • Adversely impacts a critical system or service for a subset of users. • Has a moderate probability of spreading to other systems and causing significant damage or disruption? • Username and password credentials compromised. • Stolen or lost laptop or mobile device from department with non-regulatory data • Infection of multiple computers; no regulatory data • Network fingerprinting (scanning from internal or external sources) **Response Time:** Varies **Contact:** Customer Support Center (Service Desk) (CSC), Network Administrator A post-incident report is not required but may be requested by the CISO
Low Response Level 4	• Adversely impacts a very small number of systems, services, and users. • Disrupts a very small number of systems or services; or

	• Has little or no risk of spreading to other systems and causing significant damage or disruption. • Non-descript widely broadcasted phishing campaign • Infection of single computer; no regulatory data • Machines in multiple departments infected with virus or malware or worm **Response Time**: Varies **Contact:** Customer Support Center (CSC), Network Administrators A post-incident report is not required.

4.2 Event Escalation: Response Team Communication

Once a security incident is identified and Severity and Response Levels, the TCSIRT On-Call personnel will be contacted. Which team members are activated and how quickly they need to respond is determined based on the severity of the security incident.

Multiple contacts from each group in the TCSIRT may be required to be available. The primary/secondary TCSIRT contact information list can be in a shared electronic on call calendar. If the primary contact is unavailable, the secondary contact will be attempted as soon as possible, depending on the severity of the security incident. Refer to Information Security Call List in Section 9.

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 Information County Executive
- CISO
- CPO or Privacy Officer
- Emergency Management Office
- Travis County Sheriff Office (TCSO)
- Other incident response teams within the organization
- External (contractor) incident response teams, if appropriate
- System/Application owner
- Human resources
- Legal/County Attorneys
- Law enforcement, if appropriate
- Federal government agencies, if appropriate

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

- Email
- Website (internal, external, or portal)
- Telephone calls
- In person (e.g., daily briefings)
- Conference Bridge calls
- Texting and instant messaging
- Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting)

4.3 External Communication

The CISO, or designee, will coordinate communication with the County Attorney's Office, Privacy Officer, CJIS LASO and/or PCI Compliance Officer, the affected department or elected official, and Commissioners' Court. The decision to engage outside entities will be based on the requirements specified by the relevant regulation, any applicable internal policies, and procedures, i.e. type of data, loss threshold, and certainty.

The Travis County Attorney's Office, the Commissioners Court, and affected appointed or elected official will be consulted if notification of a security incident is required to a third party other than the regulatory agency as prescribed by relevant security policy or regulation.

Circumstances that require a third-party notification include, but are not limited to:

- Evidence acquired demonstrating criminal activity
- Data breach
- Regulatory issues

4.3 Compliance and Regulatory Reporting

The TCSIR-Team will notify the CISO, Privacy Officer, CJIS LASO and/or PCI Compliance Officer (if designated) when a security incident is suspected to meet the definition of a HIPAA, CJIS, PCI, or PII breach or when the respective Officers' expertise is required to determine whether the definition could be met given the data types involved. Travis County policies and procedures related to these regulatory areas are followed once it is determined that a potential violation has occurred. See Appendix I of this plan, Reporting Data Breaches, for more information

4.4 Evidence Handling, Gathering and Storage

Should evidence of a security incident need to be collected for litigation, the TCSIRT will instruct that the affected system(s) not be touched to preserve the current state. The Travis County Sheriff's Office (TCSO) shall be notified, and Technology Operations and Security will comply with all requirements they outline. If required, a Chain of Custody document will be created for each system by the TCSIRT. This document will have the details of the collected evidence, including manufacturer, serial number, who collected the evidence and why it was collected. To maintain the data integrity, MD5 hashes of the acquired evidence may need to be taken and documented on the Chain of Custody.

A digital forensic image may be made of the original evidence if requested by TCSO. The original evidence should be handled as little as possible, stored securely with the original Chain of Custody. Any investigation that takes place would use the digital forensic image.

When not working on the digital forensic image, it and any other original evidence will need to be stored securely in a safe or limited access locked cabinet, until disposition by TCSO. The digital forensic image will be retained per statute or regulation that governs that type of information.

SECTION 5 Breach Notice Criteria

Certain types of breaches carry legal notification responsibilities. This section includes information about breach notification statutes and rules according to Texas law, federal laws and regulations, and other states' laws. ***NOTE*** As of 9/1/2017 TGC §2054.1125 requires notification of the Texas Office of the Chief Information Security Officer and the State Cybersecurity Coordinator 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.

TRAVIS COUNTY TECHNOLOGY AND OPERATIONS INFORMATION SECURITY REPORTING A DATA BREACH

5.1 Reporting a HIPAA breach

Notify the Travis County Privacy Officer
privacy@traviscountytx.gov, (512) 854-1114, or the Technology and Operations Help Desk, (512) 854-9175

Notify the HHS' Office of Civil Rights
https://www.hhs.gov/hipaa/filing-a-complaint/index.html

5.2 Reporting a PCI breach

American Express, Discovery, and Visa require you to notify them immediately upon confirming a security breach. MasterCard requires to be notified within 24 hours of knowledge.

Contact Travis County payment business partners: card brands, acquiring merchant banks and any other entities requiring notification (law enforcement, vendors, public) whether by contract or by law.

Engage with a Payment Card Industry Forensic Investigator (PFI)
https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

5.3 Reporting a CJIS breach

Contact the Travis County Sheriff's Office Local Agency Security Officer (LASO)

Please reference the FBI CJIS security Policy, Section 5.3, Policy Area 3, for further instructions.

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

5.4 Elections

The County Technology and Operations Information Security department should support the Elections Department by making revisions in the County Incident Response Plan to address requirements related to Texas Election Code Subchapter C, Chapter 129 (f) The general custodian of election records shall create a recovery plan to be followed if a breach in security procedures is indicated. This plan must include immediately notifying the secretary of state.

Table 5.1: Texas legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
Texas Identity Theft Enforcement and Protection Act (2005)	Texas Business and Commerce Code Ch. 521, §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.	Government Code §2054.1125 makes Business and Commerce Code §521.053 applicable to state agencies.

Table 5.2: Federal legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
HIPAA	45 CFR §164.404	Notify individual or Covered Entity of a breach of unsecured protected health information which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach.	Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice.

Federal Financial Participation	CMS SMDL #06-022	CMS-regulated entities must notify CMS within one clock hour according to Sep. 2006 CMS letter to State Medicaid Directors	Unclear if HIPAA HITECH eliminated the CMS requirement. SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or recipient is limited to use or disclosure "directly in connection with program administration," but have no breach notice requirement.
Internal Revenue Service	By data sharing agreement with the IRS, pursuant to IRS Publication 1075 §10	Notify TIGTA and IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals.	The IRS Office of Safeguards may require individual notification.
Social Security Administration (SSA)	By contract between SSA and Agency which defers to IRS Publication 1075	Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any.	SSA may require individual notification.
Federal Trade Commission (FTC)	Health Breach Notification (PHR, EHR Vendors) 16 CFR Part 318	Requires a vendor of personal health records to notify the individual US Citizen and the FTC following the discovery of a breach of security of unsecured PHR-identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR-related entity.	Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. "Breach" is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60 calendar days after thebreach discovery.

Family Educational Rights and Privacy Act (1974)	20 USC §1232g, 34 CFR Part 99	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.

SECTION 6 Post-Incident Checklist

1) **Learning and improving.** Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
    a. Exactly what happened, and at what times?
    b. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
    c. What information was needed sooner?
    d. Were any steps or actions taken that might have inhibited the recovery?
    e. What would/should staff, and management do differently the next time a similar incident occurs?
    f. How could information sharing with other organizations have been improved?
    g. What corrective actions can prevent similar incidents in the future?
    h. What precursors or indicators should be watched for in the future to detect similar incidents?
    i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

2) **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
    a. Creating a formal event chronology (including time-stamped information from systems).
    b. Compiling a monetary estimate of the amount of damage the incident caused.
    c. Retaining follow-up reports as specified in retention policies.

3) **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.

4) **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
    a. Reviewing of logs, forms, reports, and another incident documentation.
    b. Identifying recorded precursors and indicators.
    c. Determining if the incident caused damage before it was detected.
    d. Determining if the actual cause of the incident was identified.
    e. Determining if the incident is a recurrence of a previous incident.
    f. Calculating the estimated monetary damage from the incident.
    g. Measuring the difference between initial impact assessment and the final impact assessment; and
    h. Identifying measures, if any, that could have prevented the incident.

SECTION 7 Incident Response for OAG Data

A. Introduction

Overview

Security Incident Response is defined as an organized approach to addressing and managing the aftereffects of a security breach or attack (also known as a security incident). The goal of a security incident response program is to handle the situation in a way that limit Technology and Operations damage and reduces recovery time and costs. The following document describes the Travis County Security Incident Response Plan for handling OAG data.

Purpose

The purpose of this Security Incident Response Plan Office for Attorney General (OAG) Data supplements the Travis County ITS Incident Response Plan. Security Incident Response Plan Office for Attorney General (OAG) Data provides general guidelines on responding to security incidents effectively and efficiently by identifying, containing, mitigating, and reporting security incidents. This document guides agency response to information security incidents in accordance with federal and state rules and regulations, to include those defined in the HIPAA privacy and security standards; the Payment Card Industry data security standard (PCI DSS); and the Criminal Justice Information Services Security Policy (CJIS).

This Security Incident Response Plan is intended to provide the specific requirements that must be met to comply with the 2013/2014 State Case Registry/Local Customer Service contract.

Scope

This Security Incident Response Plan Office for Attorney General (OAG) Data applies to employees, contractors, consultants, temporary employees, and other staff members at Travis County, including all personnel affiliated with third parties conducting business on and off Travis County premises. This Plan applies to all physical and virtual equipment that is owned or leased by Travis County.

Technology and Operations Information Security Incident Response Resources

This plan is designed to be a resource reference while responding to a security incident. Other resources may be necessary to completely investigate and document a security incident, examples of which follow:

- Security Incident Response Plan
- Contact information for ISP, MSSP, AV/Malware Vendor, other 3rd party security services
- Contact information for local/state/federal law enforcement
- Current Network Diagrams
- Current Information Asset Inventory
- Disaster Response and Business Continuity Plans
- Technology and Operations On-Call/Roster information
- Compliance or regulatory bodies required reporting
- Standard Operating Procedures/ Runbooks for specific types of attacks
- General application documentation
- Policies, procedures, and standards promulgated by independently elected and appointed officials

- Current Travis County Org Chart

Definition of a Security Incident

Travis County defines a security incident as an event that actually or potentially results in adverse consequences to an information system or data that the system processes, stores or transmit Technology and Operations. Security incidents that qualify as needing the attention of the TCSIR-Team, may include, but are not limited to the following:

- Theft or loss of a Travis County computing asset
- Vulnerability exploited in an information system
- Outbreak of malicious software
- Denial of Service (DoS) attack / Distributed Denial of Service (DDoS) attack
- Unauthorized entry in Travis County applications or network
- Data Breaches for HIPAA, CJIS, Election Information, PCI or PII.
- Phish, Spear Phish, Whaling resulting in the loss of credentials
- Ransomware
- Business Email Compromise
- Authorized investigation of an insider threat

B. OAG Data Incident Management Requirements

County shall respond to security incidents involving OAG Data in accordance with Technology and Operations Information Security Incident Response Plan and specific OAG requirements as stated within this Incident Response Plan for OAG Data.

Notification Requirements

The OAG CISO and the OAG Contract Manager must be notified by telephone and electronic mail within one (1) hour of determination that OAG Data is involved in the incident. The following information will be provided to the OAG regarding details of the incident.

- Notice of incident
- Description of affected systems and networks
- Initial damage assessment
- Potential scope of the incident
- Containment/Eradication/Recovery steps taken to date
- Any changes in County contact information

Reporting Requirements

C. OAG Data Incident Management Response Process

Refer to **Section 2** for Incident Management Response Process

D. OAG Data Incident Management Post Incident Process

Refer to **Section 3** for Incident Management Post Incident Process

E. OAG Data Event Threat, Impact Analysis and Escalation

Refer to **Section 4** for Event Threat, Impact Analysis and Escalation Process

SECTION 8 Appendices

The following documents can be edited to fit your department's specific needs.

A. Incident Response Team (IRT) Charter Example

Information Privacy or Security Incident Response Team Charter

Charter Purpose:

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

IRT Mission:

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

Overview:

The Incident Response Team (the "IRT") is a standing team of internal personnel established by [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:

<u>Responsibilities:</u>

a. **Anticipate and prepare** [the agency] for privacy or security events/incidents which can be reasonably anticipated.
b. **Respond** to actual or suspected events/incidents on behalf of [the agency] as needed, with activities such as:
    i. Triage
    ii. Communication, internal and external, as needed according to [agency's] communications protocol (e.g. funneled to the top from a deputy, for example) (see communications templates)
    iii. Track and document IRT activities and discoveries; and
    iv. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

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

Roles:

1) **The IRT Lead.** The Lead of the IRT may:
    a. Be designated by and reporting to [Executive management]. The IRT is led by [_____] or his or her designee.
    b. Declare an incident
    c. Establish, maintain, and update written IRT protocols or incident response plans
    d. Identify roles and responsibilities for IRT standing members
    e. Request or designate ad hoc members for events as needed
    f. [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.

B. IRT Meeting Minutes Example

CONFIDENTIAL

Meeting Minutes for[Agency] IRT Meeting____, 20___

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

Summary
Brief incident summary:
Participants
IRT Members Present: *IRT Members Not in Attendance:* *Guests:*
Current Updates
1. 2. 3.
Prior Updates
1. 2. 3.
Next Steps
1. 2.
Next Scheduled Meeting

__:00, _. m.,____, 20____
Location:
Conference No.:_____Access Code: _____

C. IRT Action List Example

Action Items Status

Current Updates as of____.___,20____

Item	Date	Action	Assigned To	Status
1.				
2.				
3.				
4.				
5.				
6.				

D. Identity Theft Protection Criteria

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

i. Identity theft insurance with various coverages or guarantees
ii. Credit report monitoring
iii. Claims monitoring
iv. Monitoring of websites used to trade stolen information
v. Theft assistance resolution

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

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

a. Contract opportunities made available to county agencies by the Department of Information Resources for identity theft or breach management services.
b. Contractual requirements imposed upon the **Travis County** vendor or contractor, or other third party responsible for the breach, to provide identity theft protection, breach management services to the agency, or any other indemnification or hold harmless contract provisions.
c. 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.
d. 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.
e. No or low-cost measures available to impacted individuals to protect themselves, such as a self-imposed credit fraud alert, a credit freeze request to one of the credit bureaus [see breach notice template for more information] or filing a police report. Some options for impacted individuals include:
    i. A **fraud alert** which can help prevent an identity thief from opening additional accounts in a consumer's name in 90 days.

ii. A **security freeze**, also known as a **credit freeze**, which is a warning sign to businesses or others who may use an individual's credit file and requires a police report.
iii. Contacting the **Consumer Protection Division** of the Texas Office of the Attorney General.

f. The ability to link the breach event to an identity theft event or other harm.
g. The cost to the agency or agency contractor for the provision of identity theft or breach management services.

E. Example Internal Management Alert Template

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

Travis County Data Security Incident Alert

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

Summary
Brief incident summary:
Immediate Recommendations:
1. 2. 3.
Next Steps:
1. 2. 3.
Next Scheduled Update:
[Time/Day/Date or "As conditions warrant"]

F. Notice to Individuals Affected by Incident Example

<Date>

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

<<Address>>

<<City>>, TX. <<Zip>>

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

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

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

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

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

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

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

ii. The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You may contact each agency to determine if a child has a file or if the child's information has been misused:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.fraudalerts.equifax.com
Fraud Hotline (toll-free): 1-877-478-7625

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
Fraud Hotline (toll-free): 1-888-397-3742

TransUnion
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com
Fraud Hotline (toll-free): 1-800-680-7289
Report fraud: fvad@transunion.com

iii. Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.

iv. Monitor your [bank account activity / health care records / medical insurance company explanation of benefits for **Travis County Technology Operations and Security** 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 privacyofficer].

v. Report any suspicious activities on your [credit reports or bank account / health carrier 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.

vi. Learn about the Federal Trade Commission's identity theft programs by visiting 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.

vii. [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 [Agency's contracted Breach Management Vendor's] Customer Care Center toll- free at_.]

[To enroll your minor child, please call [Agency's contracted Breach Management Vendor's] Customer Care Center at_to manually enroll them. Child enrollments cannot be conducted online.]

viii. Monitor the website at [Agency's contracted Breach Management Vendor's agency / Agency's own site] for periodic updates.

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

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

Sincerely,

[Authorized signatory]

G. Public (Media) Notice Example

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

i. Brief description of the details of the event
ii. Description of the individuals affected in the aggregate
iii. Description of actions taken by the agency
iv. Statement as to whether evidence indicates the data may have been misused
v. Contact information for questions

H. Post-Mortem and Improvement Plan

INCIDENT POST-MORTEM

Cyber Incident	
Dates and Times	Indicate at a min. the start/end dates/times of the incident.
Description	Give a brief description of the incident
Impact	What was the impact to the
Detection	

Learning and Improving

Question	Response	Comment
How well did the staff and management perform?		
Were documented policy and procedures followed?		
Were the procedures adequate?		
Was the actual cause identified?		
What information was needed sooner?		
Were any steps taken that might have inhibited recovery?		
What should/would staff/management do differently the next time a similar incident happens?		
How could information sharing (in/out) with other organizations have been improved?		
What corrective actions can prevent or lower the likelihood of similar incidents in the future?		
What precursors or indicators of compromise should be watched in the		

	future to speed up detection?		
	What additional tools and/or resources are needed to address future incidents?		
	What tools, processes, metrics or resources could be in place and/or monitored to detect a similar		

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

Metrics	Enter any related metrics e.g., mean-time-to-incident-discovery, cost of recovery, time from detection to containment, …
Approximate cost of the incident	What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, agency downtime, idle employee time, backlog catchup overtime, etc.

IMPROVEMENT PLAN

This improvement plan has been developed specifically for Travis County is a result of the Cyber Incident that occurred on date.

Issue/Area for Improvement	Corrective Action	Primary Responsible	Start Date	Completion Date
Area for Improvement	Corrective Action 1			
	Corrective Action 2			
	Corrective Action 3			
Area for Improvement	Corrective Action 1			
	Corrective Action 2			

I. Security Incident Reporting Form

Technology and Operations Information Security Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Technology and Operations security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Contact Information for this Incident	
Name:	
Title:	
Program Office	
Work Phone:	
Mobile Phone:	
Email address:	
2. Incident Description.	
Provide a brief description:	
3. Impact / Potential Impact Check all of the following that apply to this incident.	
☐ Loss / Compromise of Data ☐ Damage to Systems ☐ System Downtime ☐ Financial Loss ☐ Other Organizations' Systems Affected ☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information ☐ Violation of legislation / regulation ☐ Unknown at this time	
Provide a brief description:	

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

Sensitivity of Data	
Category	**Example**
Public	This information has been specifically approved for public release by either the Commissioners Court or independently elected or appointed officials. Unauthorized disclosure of this information will not cause problems for Travis County, Technology and Operations customers, or Technology and Operations business partners. Examples are marketing brochures and material posted to Travis County web pages. Disclosure of agency information to the public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.
Internal Use Only	This information is intended for use within Travis County or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for Travis County, Technology and Operations customers, or Technology and Operations business partners. This type of information is already widely distributed within Travis County, or it could be so distributed within the organization without advance permission from the information owner. Examples are an agency telephone book and most internal electronic mail messages.
Restricted/Confidential (Privacy Violation)	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Handling of this information may be dictated by statute or regulatory body. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for Travis County, Technology and Operations customers, or Technology and Operations business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are customer transaction account information and worker performance evaluation records. Other examples include citizen data and legal information protected by attorney-client privilege.
Unknown/Other	Describe in the space provided

☐ Public ☐ Internal Use Only	☐ Restricted / Confidential (Privacy violation) ☐ Unknown / Other – please describe:

Provide a brief description of data that was compromised:

5. Who Else Has Been Notified?
Provide Person and Title:
6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken ☐ System Disconnected from network ☐ Updated virus definitions & scanned system	☐ Restored backup from tape ☐ Log files examined (saved & secured) ☐ Other – please describe:

Provide a brief description:

7. Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are non-Commonwealth systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Last Updated: Feb 2020 (P. Knight)

J. Security Chain of Custody Form

Travis County Technology and Operations Information Security Chain of Custody Form

Instructions: This form is to be completed as soon as it is determined that evidence needs to be preserved for an Information Technology (IT) security incident. All items completed should be based on information that is currently available. If you are involved in and/or working on a legal matter that involves computer hardware, software or electronic data, you should start and maintain a form for each item of evidence you handle or come into possession of. For more information, contact Technology and Operations Information Security at secops@traviscountytx.gov or the Technology and Operations Service Desk at (512) 854-9175 /HelpDesk@traviscountytx.gov.

This form may be updated and modified if necessary**.**

TECHNOLOGY AND OPERATIONS Case #	

To be completed by initial evidence collector	
Evidence collected by (name):	
Date/Time collected:	
Evidence Description:	
Describe Collection method (include operating system, utility, commands, arguments, etc.):	
What application software/utility is required to view the file?	
Where is evidence initially stored?	
How is evidence initially secured?	
Collector signature and date:	

Copy History			
Date	**Copied By**	**Copy Method**	**Disposition of original and all copies**

Transfer History	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?	
How is evidence now secured?	

Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?	
How is evidence now secured?	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?	
How is evidence now secured?	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?	
How is evidence now secured?	
Transferred from (print name, sign & date):	
Transferred to (print name, sign & date):	
Where is evidence now stored?	
How is evidence now secured?	

Last Updated: Feb 2020 (P. Knight)

SECTION 9 Contacts

External Partners. Collaboration with external entities may be necessary to assist with incident response or for auxiliary support. The TCSIRT 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 agency may need to collaborate in the event of an Incident as well as resource pages and other useful information.

9.1: 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.	Contact number: (512) 974-8631
Office of the Attorney General	The agency of the state's chief law enforcement official.	OAG main number: (512) 463-2191 Deputy Attorney General for Defense Litigation: (512) 463-0150 State Law Enforcement Criminal Investigation: (512) 936-2777 Contact OAG Information Security Officer (for Incidents affecting OAG data system or staff). Identity Theft Legal Resources and Alerts: https://www.oag.state.tx.us/consumer/index.shtml
Office of the Attorney General, Criminal Investigations Division	Investigates cybercrime and provides computer forensics services to locate and preserve digital evidence.	Criminal Investigations: CJID@oag.state.tx.us (512) 475-4220 Cybercrimes: (512) 463-9570

State Auditor's Office, Special Investigations Unit	Investigates criminal offenses affecting state resources, including computer security breaches.	Hotline: 1-800-892-8348
Texas Facilities Commission	Provides facilities services (including emergency management) for state buildings and leasing services to state agencies.	24-hour Facilities Management: (512-) 463-3600 State Leasing Services: leasing@tfc.state.tx.us (512) 463-3331
Texas Department of Information Resources, 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 Network Security Operations Center: Security-alerts@dir.texas.gov 888-839-6762 Option 1 network Option 2 Security
Texas Department of Public Safety, Emergency Management Division	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.	Division of Emergency Management Headquarters: (512) 424-2138 SOC: soc@dps.texas.gov Operations Officers: (512) 424-2208 (512) 424-2277
Texas Rangers, Texas Department of Public Safety	Leads criminal investigative responsibility for major Incident crime investigations.	Austin Headquarters: (512) 424-2160 rangers@dps.texas.gov

9.2: Federal Contacts

Resource	Services	Contact Information
Federal Bureau of Investigation	Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information.	Texas Field Offices: Dallas: (972) 559-5000 El Paso: (915) 832-5000 Houston: (713) 693-5000 San Antonio: (210) 225-6741
Federal Emergency Management Agency (FEMA)	Provides disaster response and recovery assistance.	1-800-621-FEMA (3362)
National Cyber Security Division (NCSD), US Dept. of Homeland Security	Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.	Response coordination: (202) 282-8000

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

9.3: Industry Contacts

Resource	Services	Contact Information
Ponemon Institute	Conducts independent research on privacy, data protection, and information security policy.	http://www.ponemon.org/index.php

Credit Bureaus	Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes. Consumers may request a 90-day or 7-year fraud alerts be attached to their credit bureau files by contacting one credit bureau which will in turn notify other bureaus. A credit freeze must be requested from each bureau.	Equifax: P.O. Box 740241 Atlanta, GA 30374 Fraud Hotline (toll-free): 1-877-478-7625 www.fraudalerts.equifax.com Experian P.O. Box 2002 Allen, TX 75013 Fraud Hotline (toll-free): 1-888-397-3742 www.experian.com TransUnion P.O. Box 6790 Fullerton, CA 92834 Fraud Hotline (toll-free): 1-800-680-7289 www.transunion.com Email to report suspected fraud: fvad@transunion.com Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281 1-877-322-8228 http://www.ftc.gov/freereports www.AnnualCreditReport.com
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
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/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266
Payment Card Industry – Data Security Standards (PCI-DSS)	Payment card data security standards set by the payment card industry.	https://www.pcisecuritystandards.org/security_standards/

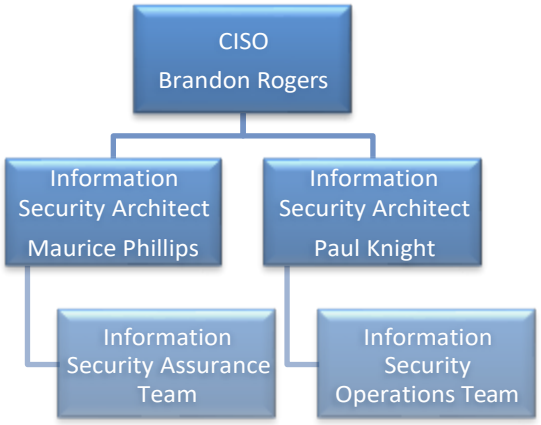
9.4: Press Contacts

Resource	Services	Contact Information
Texas Press Contacts	Texas Media Directory (subscription for distribution lists for other cities and counties).	http://www.texasmedia.com

SECTION 10

SECTION 10 Travis County Technology and Operations Contacts

10.1 Information Security Contact



Technology and Operations Information Security Team	Name	Phone	Cell Phone
CISO	Brandon Rogers	512.854.1222	512.422.6807
Security Architect	Maurice Phillips	512.854.1743	512.565.3910
Security Architect	Paul Knight	512.854.8505	512.630.4486
IT Disaster Recovery Analyst	Melissa Ojeda	512.854.1838	512.744.5582
Information Systems Auditor	Larissa Derrick	512.854.1837	512.514.3080
Sr. Information Systems Analyst	Josh Kubiak	512.854.6192	512.694.3834
Sr. Information Security Analyst	Kai Joe	512.854.1655	
Sr. Information Security Analyst	Keed Johnson	512.854.8810	
Project Coordinator	Mary Aiello	512.854.6275	
Sr. Security Analyst	Danny Cox	512.854.1839	512.773.9993
Sr. Security Analyst	Marq Hood	512.854.6762	512.589.6658
Sr. Security Analyst	Krystal Clark	512.854-4548	
Sr. Security Analyst	Jesse Ohrmund	512.854.6242	

10.2 Incident Response Team Members

Technology and Operations Security Incident Leadership Team	Name	Phone	Cell Phone
Chief Information Officer	Paul Hopingardner	512.854.8685	512.422.8607
CISO	Brandon Rogers	512.854.1743	512.422.6807
Information Technology Director	Ralph Warren	512.854.7193	
Project Management Division Director	Ernest Teves	512.854.6064	
Systems Division Director	Dain Herbat	512.854.8688	
Applications Division Director	Chris Ulibarri	512.854.4022	915.637.0498
Technology and Operations Systems Operations Manager for Customer Support	Aaron Madeley	512.854.4732	512.280.1317
Customer Support Manager	Chance Wheelbarger	512.854.6038	
County Attorney	Delia Garza	512.854.9416	

Technology and Operations Security Incident Response Team	Name	Phone	Cell Phone
Technology and Operations Systems Operations Manager for Customer Support	Aaron Madeley	512.854.4732	512.413.4331
Customer Support Manager	Chance Wheelbarger	512.854.6038	
Technology and Operations Service Desk		512.854.9175	512.632.4014
CISO	Brandon Rogers	512.854.1222	512.422.6807
Primary Contact	Paul Knight	512. 854.8505	512.630.4486
Backup Contact	Marq Hood	512.854.6762	512.589.6658
Information Technology Director	Ralph Warren	512.854.7193	
Primary Contact	Dain Herbat	512.854.8688	512.560.2204
Backup Contact	Chris Koster	512.854.1740	512.587.3287
Project Management Division Director	Ernest Teves	512.854.6064	
Primary Contact	Terry Montgomery	512.854.7784	
Backup Contact			
Application Division Director	Chris Ulibarri	512.854.4022	915.637.0498
Primary Contact	Chris Ulibarri	512.854.4022	915.637.0498
Backup Contact			

Travis County Contacts	Name	Phone	Cell Phone
TNR	Cynthia McDonald	512-854-9418	
Emergency Services	Charles Brotherton	512-854-4416	512-636-6825
Public Safety	Vicki Ashley (Interim)	512.854.4759	
Planning and Budget	Jessica Rio	512-854-4455	
Health and Human Services	Pilar Sanchez	512.854.4101	
Sheriff	Sally Hernandez	512-854-9748	
Sheriff- IT Dept. Contact			
County Clerk	Dyana Limon-Mercado		
County Clerk- IT Div Director	Scott Flom	512.854.4725	920.889.3165
Voter Registration	Gretchen Nagy	512-854-7987	

Auditor- IT Dept. Contact	Christopher Flanagan	512.854.4737	
Juvenile Courts- IT Dept. Contact	Tim Wray	512-854-7071	
Criminal Courts- IT Dept. Contact	Mark Erwin	512-854-3120	
Civil Courts- IT Dept. Contact	Michelle Hoover	512-854-2225	

External Contacts	Name	Phone	Cell Phone
City of Austin	Wendi White	512.974.1448	512.284.0539
City of Austin- Chief Information Security Officer	Shirley Erp	512.974-1465	512.217.9047
FBI	Texas Field	Dallas (972) 559-5000 El Paso: (915) 832-5000 Houston: (713) 693-5000 San Antonio: (210) 225-6741	
DIR	• Network Security Monitoring, Alerting and Analysis Services • Network Intrusion Prevention Services	DIR Network Security Operations Center: Security- 888-839-6762 Option 1 network Option 2 Security	
DIR- Deputy CISO	Jeremy Wilson		
Texas Department of Public Safety, Emergency Management Division		Operations Officers: (512) 424-2208 (512) 424-2277	
Cap Metro	Lori Hyde, Program Manager, Network Cyber Security	512-369-6553	502-594-0718
Cap Metro	Steven Salinas- Director Network Services	512-369-6544	512-590-5865
Cap Metro	Jane Schroter Vice President & CIO	512-369-6073	

SECTION 11 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; please refer to legal counsel for other relevant laws.

11.1 Texas Laws and Regulations for Data Privacy and Security

Texas Public Information Act	The Public Information Act contains provisions pertaining to information disclosure: The agency may not withhold information, even confidential information, if requested by a legislator or the Legislature for legislative purposes.	TGC § 552.008
	Information confidential by law is excepted from disclosure. Example: TGC § 2059.055.	TGC § 552.101
	Is this Incident Response Plan subject to disclosure under the Public Information Act? Some possible exceptions to disclosure for all or part of this plan:	
	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
	Network security is exempted from the requirement to disclose in the Public Information Act.	TGC § 552.139, TGC § 2054.055, ORD 581 (1990)
	Are records relating to the breach Technology Operations and Security 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, TGC § 552.024, TGC § 552.117
	Information related to litigation, if pending or reasonably anticipated, is exempt from disclosure.	TGC § 552.103
	Information related to competition or bidding, generally while bidding is in process, is exempt from disclosure.	TGC § 552.104, TGC § 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)).	TGC § 552.107, TGC § 552.022(b)
	Certain law enforcement records may be kept private, generally while the case is pending.	TGC § 552.108
	Trade secrets are exempt from public disclosure.	TGC § 552.110
	Agency memoranda which would not be made available to a party in litigation (including attorney work product) are exempt from disclosure.	TGC § 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, ORD 684 (2009)
	Email addresses of the public are exempt from disclosure.	TGC § 552.137
	Social security numbers are exempt from disclosure.	TGC § 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 Technology Operations and Security 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
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	BCC Ch. 521

	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.	
Texas Medical Records Privacy Act	The Texas Medical Records Privacy Act is Texas law making Protected Health Information 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
Texas Administrative Code	Information Security Standards for State Agencies and Institutions of Higher Education.	1 TAC 202
	Administrative rule pertaining to agencies' websites.	1 TAC 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, 1 TAC § 206.72
	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(W)

11.2 Federal Laws and Regulations for Data Privacy and Security

Health Insurance Portability and Accountability Act (HIPAA) (1996)	HIPAA contains the following provisions regulating the use and disclosure of protected health information: • *Privacy Rule* protects the privacy of individually identifiable health information. • *Security Rule* sets national standards for the security of electronic protected health information;	HIPAA (1996);

	• *Breach Notification Rule* requires covered entities and business associates to provide notification following a breach of unsecured protected health information. • *Enforcement* providing civil and criminal penalties for violation; and • *Patient Safety Rule* protects identifiable information being used to analyze patient safety events and improve patient safety.	
Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)	HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA Business Associates and requiring Covered Entities and Business Associates to report data breaches to those affected individuals through specific breach notification requirements.	HITECH (2009) (ARRA Title XIII)
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; and • Finalized rule adopting GINA and prohibited most health plans from using or disclosing genetic information for underwriting purposes, as proposed in Oct. 2009.	45 CFR Parts 160-164
Family Educational Rights and	FERPA creates a right of privacy regarding grades, enrollment, and billing information. Specifically, this information may not be released without prior consent	20 USC § 1232G; 34 CFR Part 99

Privacy Act (FERPA) (1974)	from the student. In addition to safeguarding individual student records, the law also governs how state agencies transmit testing data to federal agencies.	
Federal Information Security Management Act (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 **(FISMA)** information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to drive down Technology and Operations security issues effectively and efficiently 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 Technology Operations and Security 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
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; IRC Section 6103(p)(4); 26 USC §6103(p)(4)
Social Security Administration (SSA) Statute and Regulation	Much of the information SSA collects and maintains on individuals is especially sensitive, therefore prior to disclosing of 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 1974; 5 USC Section 552a; FOIA; 5 USC §1106 (SSA); 42 USC §1306

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 subset of the controls. Agencies are expected to comply with NIST security standards and guidelines.	NIST 800-53 rev. 4; FIPS 200
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 Technology Operations and Security 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, TGC § 552.108
Clinical Laboratory Improvements Amendments (CLIA)	CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services.	CLIA Regulations and Guidance

Computer Fraud and Abuse Act (CFAA)	CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines "protected computers" as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication.	18 USC §1030

Enforcement Action

The CISO, Privacy Officer, or County Attorney (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), as applicable, for appropriate 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.

The agency will cooperate with appropriate law enforcement if any user may have violated federal or state law.

Acknowledgements

Version 2 of the Incident Response Plan was published on behalf of Travis County Technology Operations and Security with the guidance from the Department of Information Services (DIR).

The current version of this document is maintained by the Travis County Technology and Operations Information Security Office.