Information Security Policy Manual

November 2017

Manual Notice 2017-1

From: Terri Duncan, Information Security Officer

Manual: Information Security Policy Manual

Effective Date: November 15, 2017

Purpose

This manual issues policies for TxDOT's information security functions and creates a dynamic program that protects the confidentiality, integrity, and availability of TxDOT's information resources. This manual consolidates information security policies currently published on several TxDOT websites. New policies are published publicly and made available only through the TxDOT Manuals system.

Contents

The new *Information Security Policy* manual contains five policy statements and their objectives. Chapter 1 provides an introduction, basis of authority, and defines the intended audience. The policies are covered in Chapters 2 through 6. Each chapter starts with the policy statement then

- identifies objectives that support the policy
- outlines minimum protocol for meeting objectives
- assigns responsibilities based on functional roles.

Supersedes

The policies in this *Information Security Policy* manual supersedes all prior policy statements on information security, including:

- TxDOT Policy Statement 2-96
- TxDOT Information Security Manual, issued with Manual Notice 2012-2
- Security policies published on SharePoint sites.

Applicability

The policies in this manual apply to **all** individuals who use or maintain TxDOT-owned data and systems while employed or contracted with TxDOT, regardless of work location. Individuals are responsible for complying with the intent and objectives as described in this manual.

Contact

Questions about the policies or their applicability may be directed to: IMD-Security@TxDOT.gov. TxDOT's Information Security Officer (ISO) is the chief decision maker for all security related issues. Only the ISO or delegate can address questions on information security policies and how those policies are to be carried out.

Archives

This is a new manual. No archives exist.

Table of Contents

Chapter 5 — Investment Protection

Chapter 6 — Business Continuity

Chapter 1 — About Information Security Policies

Contents:

Section 1 — Overview

Policy Overview

Five policy statements define how TxDOT protects its information resources and the systems in which they reside. These policies establish the intention to

- meet state and federal regulations
- protect assets
- support business goals.

Security Framework. References to the five objectives of the *Texas CyberSecurity Framework* (Identify, Protect, Detect, Respond and Recover) appear throughout this manual. These references further illustrate how TxDOT policy objectives align with statutory requirements. The protocol and general responsibilities listed under each objective include industry best practices as well as guidelines established by the National Institute of Standards and Technology, NIST.

Manual Intent

This manual establishes the policies to govern TxDOT's Information Security Program and describes the objectives of each policy. Each objective includes a subsection on the protocol and general responsibilities of individuals who use information resources.

This manual **does not** intend to be a comprehensive approach for administering TxDOT's Information Security Program. Authorized individuals who have a greater operational interest in TxDOT's Information Security Program may also read the additional manuals pertaining to the program. Those are described at the end of this section.

Intended Audience

The policies in this manual apply, at all times, to individuals who use TxDOT-owned information and systems while employed with TxDOT, regardless of work location. These policies also apply to systems, tools, and methods used to conduct business on behalf of the Agency. Individuals who use TxDOT information resources are required to familiarize themselves with the policy statements, their objectives, and the general responsibilities listed. The "Additional Focus Areas" table shows functional job descriptions that carry additional work responsibilities:

Additional Focus Areas

IF you...	Become familiar with the policy and objectives of...
use TxDOT-owned information, equipment, or networks	Security Awareness

Additional Focus Areas

IF you...	Become familiar with the policy and objectives of...
are business owners or involved with the daily operations of a functional business process, also known as information owners and information custodians	◆ Security Awareness ◆ Intrusion Prevention ◆ Information Quality and Integrity ◆ Business Continuity
work to support information technology projects, acquisitions or improvements	◆ Security Awareness ◆ Information Quality and Integrity ◆ Investment Protection ◆ Business Continuity
administer TxDOT-owned information, equipment, or networks or work in the Information Management Division	All the policies and their objectives

Violations of the information security policies or misuse of TxDOT information resources may result in disciplinary actions, including termination and legal prosecution. Questions about the policies or their applicability may be directed to: IMD-Security@TxDOT.gov. Only TxDOT's Information Security Officer can issue information security policies.

Terminology

As much as possible, the manual avoids using industry-specific terminology. When technical terms are necessary for accurate discussions, definitions are provided within the paragraph.

Equivalent Titles

The “General Responsibilities” subsections under each policy objective also list the functional responsibilities the Texas Information Security statutes assign to generic business roles. Definitions for each of the roles are available in 1TAC§202.1. While TxDOT does not use these generic titles, TxDOT does provide equivalent, specific business roles. The information below maps the term used in the statute to their TxDOT counterparts:

Agency Head—The Agency Head is TxDOT’s Executive Director

Information Custodian—Information Custodian is the person or group responsible for the day-to-day functions of a designated business process and who has access to a TxDOT information asset. For example, the custodian is the person who directly works with the information.

Information Owner— Information Owner is an individual who is the designated owner of a specific business process. For example, this may be a section director, lead worker, or business analyst as long as that person is the **named** decision-maker for the business operations that use the information.

User of an information resource— User of an information resource is an authorized TxDOT employee, contractor, partner, customer, guest, who has been granted privileges to gain access to the agency's information systems and their data. The user of an information resource may be another automated system.

Section 2 — Implementation and Authority

Implementation

TxDOT uses a risk management approach to balance business productivity with data and infrastructure asset protection. TxDOT's Executive Director delegates authority and responsibility for this approach to the Information Security Officer (ISO), who directs the Information Security Program. Along with the policies issued in this manual, the ISO:

- governs the security processes to implement these policies
- identifies the procedures to carry out the processes
- establishes the standards by which implementation of the policies is measured
- monitors the effectiveness of each process and makes adjustments as necessary
- verifies that process results meet established standards
- validates results
- reports on the Information Security program status.

Basis of Authority

Content in this manual is based in several federal and state laws and on existing agency policy.

- *Texas Administrative Code*, Title 1, Chapter 202 Information Security Standards
- *Texas Penal Code*, Chapter 33, Computer Crimes
- *Texas Business and Commerce Code*:
  - Chapter 322, Uniform Electronic Transactions Act
  - Chapter 521, Unauthorized Use of Identifying Information
- *Texas Government Code*:
  - Chapter 403, Section 275, Liability for Property Loss
  - Chapter 552, Public Information
  - Chapter 2054, Information Resources
  - Chapter 2203, Requirement to Use State Property for State Purposes
- *Texas CyberSecurity Act*, HB8, 85th Regular Session
- Federal laws, including:
  - *Computer Security Act of 1987*, Public Law 100-235
  - *Electronic Signatures in Global and National Commerce (ESIGN) Act*, Public Law 106-229

- *Computer Fraud and Abuse Act of 1986* Title 18, *U.S. Code*, Section 1030

NOTE: Order of Precedence. Legal authorities, such as federal or state laws and regulations take precedence over TxDOT policy if a conflict arises. However, TxDOT policy will take precedence over best practices, industry standards, and National Institute of Standards and Technology (NIST) guidelines.

Section 3 — Maintenance Cycle

Review Cycle

The *Information Security Policy* manual will be reviewed on a yearly basis. When updates are needed they will be issued with a manual notice and be published in the Online Manual system. Send an email to IMD-Security@TxDOT.gov to subscribe to update notices.

Additional Manuals

While this manual provides general directions for information security policies, five other manuals provide detailed discussions for information security:

- *Information Security Standards* manual provides the minimum requirements necessary to remain in compliance with the policies explained in the *Information Security Policy* manual.
- *Information Security Governance* manual is for all business units. It provides broad guidance and reasoning on what to consider in the decision-making process.
- *Information Security Program* manual is based on the *Texas CyberSecurity Framework* and connects day-to-day operations requirements with TxDOT's five policies. This manual is a **confidential** resource for technically-inclined readers.
- *Information Security Incidents* manual lists the specific standards and techniques TxDOT must meet to detect, respond to, and recover from breaches. Like the Program manual, it is confidential and written for technically-inclined readers. Its distribution **is limited** to individuals who have a need to know, only.
- *Information Security Awareness* manual provides requirements and references to acceptable sources that help readers increase their awareness of security issues such as phishing connections, man-in-the-middle schemes, and denial of service attacks. It is written for a wide audience.

Chapter 2 — Security Awareness

Contents:

Section 1 — Security Awareness Policy

Policy Statement

TxDOT's **Security Awareness Policy** is to foster an environment where individuals can make knowledgeable decisions to keep information secure and to protect the data and systems TxDOT uses. The intent of the policy is to increase attention to potential threats, enabling TxDOT's work-force—permanent, temporary, and contracts—to avoid behavior that could put agency information and systems at risk.

Objectives

The five objectives of the Security Awareness policy are to:

- improve the use of passwords including
  - their complexity
  - frequency of change
  - confidentiality
  - reporting of compromised passwords
- incorporate planning for security measures in projects
- purchase necessary components and services to safeguard information assets
- use information resources wisely
- create a security awareness and training program.

Each of these objectives is discussed in the following sections of this chapter. Each section provides a brief introduction of the objective, discusses the minimum protocol TxDOT must follow, and assigns responsibility for the required work.

Section 2 — Using Passwords

Introduction

This section describes how to improve the use of passwords as an objective of the **Security Awareness** policy. Improving the effectiveness of passwords provides an individual-based approach to the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

Minimum protocols and responsibilities must be in place to effectively create, use, and maintain secure passwords that reduce the risk of unauthorized access. Paramount among these is the confidentiality of all passwords. Individuals who suspect their password has been compromised must first create a new password and then report this suspicion through TxDOTNow.

Categories.TxDOT uses passwords to verify the level of access privileges granted to its network. All account passwords must conform to the standards established for each type of account. TxDOT will use Single Sign-On methods for individual user accounts whenever possible to reduce managing multiple passwords.

Expiration. Passwords must be changed periodically. Default passwords must be changed before accessing TxDOT's network.

Responsibilities

All individuals who use TxDOT's information technology and the data it contains must:

- use the appropriate password standards for the type of account to allow the correct level of authentication.
- conform to the password management practice established in the Information Security Program.

NOTE: Use the Exception Request Process to request an exemption to this policy. IF granted, the exemption must be included in the TxDOT Risk Register.

Compliance and Standards

See the "Password Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Security Awareness Policy**.

Section 3 — Planning for Security

Introduction

TxDOT's Information Security Office manages the planning process for security controls to enable business functions while managing risks. This effort links the Agency's security program with its Strategic Plan. Linking security controls with the Strategic Plan aids project teams to coordinate security concerns as they develop automated business solutions. Planning and managing security controls allows for greater integration with the Strategic Plan and addresses the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT centrally manages the Information Security planning process to assess the need for, authorize the use of, and monitor the effectiveness of security controls and processes. This effort is integrated in the development process and applies to all applications, systems, and projects throughout their life cycle.

General Responsibilities

TxDOT uses federal and state laws and regulations to shape its Information Security policies, including adopting the National Institute of Standards and Technology (NIST) Special Publications standards and the Texas Department of Information Resources (DIR) Control Catalog. All individuals who use TxDOT information resources must adhere to these policies. Unique responsibilities for these policies are identified and discussed below.

Agency Head. As the agency head, TxDOT's Executive Director is responsible for the Agency's information resources and designates an Information Security Officer to administer the Agency's Information Security program. Additionally, the Executive Director sanctions the program by allocating resources, ensuring collaboration from senior agency officials, reviewing the program annually, and ensuring the program's management processes are integrated with the TxDOT strategic and operational planning processes.

Information Security Officer (ISO). The ISO specifies the security requirements for the Agency. The ISO creates the Agency's security plans, policies, and procedures; and ensures that security training is available for individuals who use TxDOT information resources. The ISO is the chief source who can issue exceptions to security requirements, provided they are justified, documented, and included in the Agency's Risk Management and Assessment process.

Compliance and Standards

See the "Planning Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Security Awareness Policy**.

Section 4 — Acquiring Systems and Services

Introduction

This section establishes how TxDOT reduces the inherent risks in buying information technology equipment or services. As part of the Security Awareness Policy, this section provides a list of topics to consider. These topics ensure security controls are considered when the purchase is made. These considerations address the "Protect" objective of the Texas CyberSecurity Framework.

Protocol

TxDOT follows the National Institute of Standards and Technology (NIST) principles for Information Security System and Services Acquisition. These principles advise agencies to follow industry best practices, plan for purchasing information resources, integrate security activities into the project or program lifecycle, document and understand the security configurations, and follow all applicable laws.

General Responsibilities

Individuals who purchase IT products or services must obtain documentation to

- show the chain of supply, including origin, delivery, and support methodologies
- confirm that the vendor's personnel have each met the terms and conditions of TxDOT pre-employment personnel assessment processes and procedures
- secure confidentiality of TxDOT information
- demonstrate compliance with security controls and requirements.

Compliance and Standards

See the "Acquiring Systems and Services" standard in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Security Awareness Policy**.

Section 5 — Using Information Assets in Acceptable Ways

Introduction

This section establishes how TxDOT protects its information assets from inappropriate uses to reduce risks, such as: exposures to virus attacks, compromising of network systems and services, and legal issues. As part of the **Security Awareness Policy**, this section lists topics to consider and behavior to avoid. Both ensure that individuals approach using technology and information assets with security considerations in mind and support the "Protect" objective of the Texas CyberSecurity Framework.

Protocol

TxDOT will protect its information resources from unnecessary risks by monitoring activity, separating business traffic from guest traffic, limiting the devices that connect to the network, and ensuring that software and devices on its network are owned and appropriately licensed to TxDOT. Paramount to this effort is each individual's understanding and compliance with this section. TxDOT does provide a Guest network that allows individuals access to personal information on personal devices while on TxDOT property. The Guest network is subject to the same monitoring activity to ensure TxDOT information assets are protected. *Texas Government Code §2203.004* prohibits the use of state property for anything other than state use.

Individuals who have a business need to access TxDOT information must complete Form 1828A, *"Information Resources Security Compliance and Confidentiality Agreement"* to verify they have received the Agency's direction on the confidentiality of its information and its acceptable uses.

General Responsibilities

Individuals who use TxDOT information resources must:

- use the state resources only for state business
- comply with all the security controls established by Agency policies, processes, and procedures
- report theft, loss, or unauthorized disclosure of information
- provide written acknowledgment that they will comply with this policy in the prescribed manner.

Individuals, including those with Administrative rights, who use TxDOT information resources must not:

- disable required software

- conduct illegal activities
- violate TxDOT policies
- release information assets without authorization.

Compliance and Standards

See the “Acceptable Use Standards” in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Security Awareness Policy**.

Section 6 — Training to Increase Security Awareness

Introduction

This section explains how TxDOT will increase attention to potential threats, enabling individual users of Agency information resources to avoid behavior that could put its information systems at risk. As part of the **Security Awareness Policy**, this information provides the parameters to establish an awareness and training program to boost the "Protect" objective of the Texas CyberSecurity Framework.

Protocol

TxDOTsecurity awareness and training program provides:

- initial access to those who have a legitimate reason to be on the TxDOT network
- role-based, specific training for those who have elevated duties, privileges, and authority, including the individuals who manage, administer, operate, and design IT systems
- periodic updates and notification of evolving security practices.

Threat Awareness Program. TxDOT will implement a threat awareness program that includes cross-organization information sharing capability.

General Responsibilities

All individuals who use TxDOT information resources must complete the Security Awareness training within a reasonable time of receiving a unique identifier, commonly known as a user ID, and access to Agency resources. Additionally, the following roles have specific responsibilities:

Information Security Office. Office staff must collaborate with the Workforce Development staff to create and update

- baseline Security Awareness training programs for **all** individuals who access Agency information resources.
- intermediate Security Awareness training programs for Information Owners and Information Custodians, as defined in Chapter 1, Section 3.
- advanced Security Awareness training programs for publication specialists who are tasked with releasing information to the general public, regardless of the medium.

Both the Information Security and Workforce Development staff collaborate to deliver these training programs on a periodic basis.

Compliance and Standards

See the "Training Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Security Awareness Policy**.

Chapter 3 — Intrusion Prevention

Contents:

Section 1 — Intrusion Prevention Policy

Policy Statement

TxDOT's **Intrusion Prevention Policy** is to establish a complex, layered, and overlapping approach that leverages people, processes, and technologies to monitor the environment, assess threats, and identify weaknesses. The intent of the policy is to protect information assets by verifying that individuals have authorized access and by preventing intentional and accidental use of TxDOT information throughout its lifetime, regardless of its location.

Objectives

The Intrusion Prevention Policy has seven objectives aimed at preventing individuals with negligent or fraudulent behavior from abusing information assets. The objectives of this policy are:

- identify users and verify their authenticity
- control access
- protect the virtual perimeter
- monitor security efforts
- filter out malicious content
- conduct assessments to determine vulnerabilities and adjustments
- use cloud-based services safely.

Each of these objectives is discussed in the following sections of this chapter. The discussions provide a brief introduction of the objective, list the minimum protocol TxDOT must follow, and assign the responsibility for the work.

Section 2 — User Identification and Authentication

Introduction

TxDOT will identify individuals and verify their identity before allowing access to its information assets. This section addresses the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT will uniquely identify each individual and manage this information through processes that identify and authorize individuals, groups, roles, or devices as the valid user of a specified set of credentials before any access to TxDOT information resources is granted.

Authentication. This process of verifying the validity of a set of credentials is commonly known as authentication. TxDOT uses several means to verify the identity and authorize access, including: multi-factor authentication for local and remote network access; system authenticators; and token- and password-based authenticators.

Management. TxDOT will establish, implement, and refine procedures for:

- distributing initial authenticators
- changing default content on first use
- protecting authenticator content from unauthorized disclosure and modification
- establishing thresholds for life time restrictions and reuse conditions
- replacing lost, compromised, or damaged authenticators
- revoking authenticators.

General Responsibilities

All individuals who use information resources must provide correct identification and authentication in order to gain access to TxDOT's information systems.

Supervisors must validate the identity of individuals requesting access to TxDOT's information systems.

Information Security Officer must:

- implement security controls to correctly identify and authenticate individuals
- ensure that all individuals who use TxDOT information resources comply with the identification and authentication mandates issued in the **Intrusion Prevention Policy**.

Compliance and Standards

See the "Identification and Authentication Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Section 3 — Access Control

Introduction

Controlling access into a system (internal or external to the agency, wired or wireless, on premises or remote) provides necessary protection for information assets and the environment in which they reside. There are multiple ways to protect these points of entry. Commonly known as access controls, these protections allow entry only to individuals or systems with prior approval who have a declared need, and to whom access has been extended. TxDOT uses multiple tools in various formats—physical and virtual locks—to authorize entry. This section establishes how TxDOT uses access control as part of its **Intrusion Prevention Policy** and describes the minimum protocols and responsibilities that must be in place to effectively control access. It provides a system-based method to address the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT will safeguard information assets and the environments where they are stored. This includes controlling access as well as the flow of information. Controlled access can be both physical and logical. Examples of physical access include posting security guards at building entrances while an example of logical access is designating user identification (IDs) for login into the TxDOT network. Controlling the flow of information includes allowing individuals on a system and allowing systems to read and write to one another through their connections. Control mechanisms must be applied to applications, servers, databases, and network devices. Examples of these mechanisms already in use at TxDOT are session limits (such as a web page expiring), lockout features (requires authenticated individual to log in again after a defined period of inactivity,) and account expirations (such as passwords needing to be reset after a designated amount of time).

Notification. Electronic forms and notices on systems, commonly called "splash screens," let individuals know about applicable laws, statutes, and agency policies. TxDOT provides a system notice to all individuals and maintains signed access agreements and similar documentation as stipulated in its *Records Retention Schedule*.

Types of Access. TxDOT follows the principle of Least Privilege, regardless of the type of access an authorized person or system seeks. This principle designates that the access granted will not exceed the necessary allowances required for specific duties or tasks. For example, a system that must read information from a secondary source will not be allowed to write information to the secondary source. This principle applies to all types of access including remote access, media access, external access, service accounts, and even physical access such as badged entries.

Remote or External Access. All remote and external access to the network must occur through a virtual private network, commonly referred to as a VPN. Often described as a secured tunnel, VPNs

allow authorized individuals to extend a secured network onto a public network. The tunnel protects the information that travels inside of it. Public services must be used outside the network perimeter. External devices trying to connect to the network can be assessed for potential threats before they are allowed inside the perimeter.

General Responsibilities

All individual users of TxDOT information resources must remain in compliance with the access control boundaries. Certain key roles have additional responsibilities listed below.

Administrators. Individuals and business units who administer TxDOT servers, networks, domains and applications must:

- grant access on the principle of least privilege when both the:
  - the information owner has authorized an individual to gain access and
  - individual consents to adhere to all of TxDOT's information security policies.
- maintain lists of all domains, groups, and individuals with authorized access to TxDOT's information environment
- maintain a list of all interfaces
- maintain access logs for auditing purposes
- notify individuals of externally facing systems that they are on a TxDOT asset used for state business
- inform the Information Security Office when resources are out of compliance with policy

Information Owners. The designated owners of business processes must:

- authorize access rights
- grant access rights to individuals who consent to all of TxDOT's information security policies.
- bases access rights according to the Principle of Least Privilege
- classify information to determine what security controls are necessary to best protect it.

Information Security Officer must:

- oversee and implement security controls within TxDOT information systems
- ensure external information systems containing TxDOT information meet intrusion prevention protection that is equivalent to this policy
- ensure individuals comply with the access control boundaries issued in the Intrusion Prevention Policy.

Compliance and Standards

See the “Network Access Standard” in the *Information Security Standards* manual for a a list of the minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**

Section 4 — Perimeter Control

Introduction

Much as a fence with a locked gate can control who goes in or comes out of an area, a secure perimeter around TxDOT's network can reduce the exposures of unwanted intrusions. Both, physical or virtual fences, must have the proper configurations to keep out trespassers. TxDOT is committed to reducing its exposure to potential threats while ensuring authorized individuals have the functionality necessary to perform legitimate business. This section establishes how TxDOT will control its perimeter as part of its **Intrusion Prevention Policy** and describes the minimum requirements that must be in place to regulate access to its network. This objective provides a boundary-based approach toward the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT takes precautions, through a variety of mechanisms, to safeguard its network perimeter. These precautions include following the principle of Least Functionality; configuring protection devices to deny entry; and using only secured methods to gain access to the network. TxDOT conducts frequent perimeter checks, minimally once per quarter, to identify and disable unnecessary or non-secure functions, ports, protocols or services.

Least Functionality. The principle of Least Functionality limits access to only the amount needed for employees to complete routine job functions. Limiting functionality prevents individuals from maliciously or accidentally exploiting enabled functionality that is unused.

Deny all, allow only by exception rule. Security devices aimed at protecting the perimeter must be configured so that all entry requests are denied unless explicit entry permission is granted. Examples of these devices include firewalls, border routers, intrusion detection systems, and intrusion prevention systems. Additionally, software or applications must have prior approval before use of these connections.

General Responsibilities

Individuals who use TxDOT information resources must remain in compliance with Perimeter Control boundaries. Certain key roles have additional responsibilities listed below.

System Administrators must:

- ensure all device configurations TxDOT standards
- perform quarterly reviews of the perimeter defenses
- report review findings to the Information Security Office.

Information Security Officer must:

- review all information systems configurations
- provide authorization to operate for all information systems
- ensure all individuals who use TxDOT information resources comply with the perimeter control boundaries issued in the Intrusion Prevention Policy.

Compliance and Standards

See the "Network Perimeter Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Section 5 — Security Monitoring

Introduction

Monitoring and logging all security events and incidents provides TxDOT the ability to recognize, react to, and mitigate actions that threaten to disrupt the availability and integrity of TxDOT information assets. The information provided in this section is part of the Agency's **Intrusion Prevention Policy.** It addresses the "Detect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT strategically deploys monitoring devices to detect when physical access to its information resources occurs. The information collected from security incidents and events must be retained according to the *Records Retention Schedule*. TxDOT will use real-time monitoring to:

- assess the information and data transfers to and from TxDOT's network
- monitor the health of its equipment, including currency of hardware and software.
- determine if unauthorized access has occurred
- analyze how the information movement correlates to risk assessments and security plans.

General Responsibilities

Individuals who use TxDOT information resources must monitor both physical and digital access, use, and health of the information resources they use. Any security incident or event detected must be immediately forwarded to TxDOT Information Security Office for response and mitigation.

Information Security Officer must ensure that:

- information owners and custodians adhere to TxDOT's security monitoring standards
- incidents and events are evaluated and mitigated according to the risk management framework
- individuals comply with the security monitoring standards issued in the Intrusion Prevention Policy.

Compliance and Standards

See the "Security Monitoring Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Section 6 — Internet Content Filtering

Introduction

The inherent risks of conducting state business over global, public networks reinforce the need for careful, deliberate filtering of Internet content. This content includes email, telephony, video, web services, web browsing, and file transfers. Recognizing, then separating, potential threats from authorized individuals aligns with the Agency's **Intrusion Prevention Policy** and helps to implement the "Detect" objective of the *Texas CyberSecurity Framework.*

Protocol

TxDOT will filter digital communications using multiple mechanisms. This allows TxDOT to gain the greatest protection and target its defensive efforts. For example, email traffic often contains spam, phishing attacks, and malicious hyperlinks. These communications and web activity will be monitored for the proper use and authorized access to TxDOT information resources.

General Responsibilities

Those who use TxDOT information assets must follow the rules included in the Acceptable Use Form they signed to gain access to TxDOT's network. Information custodians, information owners and the Information Security Officer have additional, specific responsibilities listed below.

Information custodians ensure the information within their assigned purview is monitored and filtered when it passes to and from TxDOT's network.

Information owners select and manage information that may use a cloud service provider.

Information Security Officer must:

- provide to information owners, custodians, and individuals support for the safe use of web services and email filtering
- implement security controls for filtering web and email content to prevent data loss
- ensure that information owners and custodians comply with the Internet content filtering mandates issued in the Intrusion Prevention Policy.

Compliance and Standards

See the "Internet Content Filtering Standards" in the *Information Security Standards* manual for minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Section 7 — Vulnerability Assessments

Introduction

All TxDOT information systems undergo vulnerability assessments to help and correct flaws that leave them open to attack. This specifies how often these assessments are conducted and how their findings are addressed. Conducting vulnerability assessments aligns with the Agency's **Intrusion Prevention Policy** and helps implement the "Detect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT conducts vulnerability assessments on a quarterly rotation for all information resources deployed on its network. The purpose of the quarterly rotation is to ensure all assets are assessed for vulnerabilities on a yearly basis. The assessments are conducted specifically to identify, analyze, and report flaws

- on the network
- in application configurations that are either on or off the network
- in the source code for web applications and services, databases, software, and mobile applications.

TxDOT conducts these evaluations within a centrally-managed vulnerability assessment system.

General Responsibilities

Assessment of vulnerabilities is the joint responsibility of the Information Security Office and the Office of Primary Responsibility for the asset, product or service being evaluated. Employees must cooperate with the vulnerability assessments and with the Information Security Office to correct any flaws.

The Information Security Officer ensures that employees comply with the vulnerability assessments mandates issued in the Intrusion Prevention Policy.

Compliance and Standards

See the "Vulnerabilities Scan Standards" in the *Information Security Standards* manual, for minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Section 8 — Cloud Usage

Introduction

Selecting the appropriate virtual environment for computing resources is the first critical step in procuring secure cloud services. Cloud services includes both the hosting of content on a virtual network and accessing the service through an Internet connection. This section establishes how TxDOT uses these services as part of its **Intrusion Prevention Policy** and describes the minimum protocols and responsibilities that must be in place. It specifies and defines what considerations to address, aligning the discussions with the "Identify" objective of the *Texas CyberSecurity Framework*.

Protocol

Regardless of the service provider or the type of cloud-based service sought, TxDOT shape service agreements that specify the appropriate levels of service, the standards for the service, and how TxDOT information assets are protected. Customarily, Texas State agencies seek cloud services through the Texas Data Center Services. The Texas Department of Information Resources (DIR) may grant exceptions for alternate cloud service providers (CSP) when business reasons are justified. These services include Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).

General Responsibilities

TxDOT employees and contractors seeking a cloud-based solution must carefully define the roles and responsibilities among all the service providers and TxDOT to effectively manage cloud-based services that are of benefit to the Agency. This collaboration with a potential provider must fully:

- integrate all terms of service in the contract.
- define performance with clear terms and definitions; demonstrate how to measure performance; and create enforcement mechanisms that allow for service adjustments when necessary.
- detail the security requirements to maintain the confidentiality, integrity, and availability of cloud-based information assets.
- identify both the use of National Institute of Standards and Technology and TxDOT standards for cloud architecture.

Those who seek a cloud-based solution must also address potential privacy risks, legal discovery, and electronic records management and disposition in keeping with all applicable laws and regulations.

Information custodians must ensure proper administration of cloud services as specified in the agreements between TxDOT and the cloud service provider.

Information owners help to select and manage the information assets residing with a cloud service provider.

Information Security Officer must ensure individuals and cloud service providers comply with the cloud usage mandates issued in the **Intrusion Prevention Policy.**

Compliance and Standards

See the "Cloud Standards" in the *Information Security Standards* manual for the minimum standards necessary to comply with this objective of the **Intrusion Prevention Policy**.

Chapter 4 — Information Protection

Contents:

Section 1 — Information Protection Policy

Policy Statement

TxDOT's **Information Protection Policy** ensures a balance between using information and protecting its quality and integrity to allow for the optimization, maintenance, and disposition throughout the informations' lifetime. The intent of the policy is to protect information assets, regardless of their location (either on premises or as cloud-based services) or its state (at rest or in processing).

Objectives

The Information Protection Policy has five objectives to guard its information from accidental or purposeful corruption or other misuse. The objectives of this policy are to:

- classify data
- encrypt data
- use digital signatures safely
- safeguard privacy
- ensure system and information integrity

Each of these topics is discussed in the following sections of this chapter. The explanations provide a brief introduction of the topic, lists the minimum protocol TxDOT must follow, and assigns the responsibility for the work.

Section 2 — Classify Data

Introduction

This section establishes how TxDOT classifies data as part of its **Information Protection Policy** and describes the minimum protocols and responsibilities that must be in place to effectively assess the value of information against the risk of it being misused. It provides a dynamic approach to the "Protect" objective of the *Texas CyberSecurity Framework.*

Protocol

TxDOT owns all the data created and used in support of its business activities. The offices responsible for identifying and prioritizing department needs associated with the data must classify the data into three categories: public (least restrictive), sensitive, and confidential (most restrictive).

The data is classified either by the content itself or by its system **after** considering the damage that could occur to individuals or TxDOT if the information were used for something other than its original purpose. All TxDOT information—regardless of form, format, quantity, or location (on or off premises)—must be classified.

Considerations must also include:

- where the information is initially created or captured, processed, transferred, kept, archived, and disposed
- form of the data -- whether it is physical (a hand-written note) or digital (an email) is not relevant, and it must still be classified
- the data's context. For example, a common individual name may not pose any risks until it is paired with a social security number, street address, date of birth, etc. to identify a specific person, vulnerable to suffering damage.

To help assess the significance of the misuse, TxDOT will **both** use the "Potential Impact Definitions for Security Objectives" published by the National Institute of Standards and Technology (NIST), **and** these factors:

- value and associated risks of the data
- levels of protection as required by state and federal laws
- obligations as stewards such as ethical, proprietary, and privacy protection.

When considering those factors, TxDOT must:

- recognize that data classifications are subject to change

- review data periodically to ensure it meets current classification levels
- protect backups with the same classification level provided for the original data
- employ sanitation mechanisms with strength and integrity commensurate with the security category of the information.

Responsibilities

General. The responsibility for protecting the data varies according to the role employees play in creating, maintaining, using, and storing the information. These roles are defined in Title 1, Part 10 of the Texas Administrative Code, Chapter 202, Subchapter A, 1TAC§202.1. Minimally, individuals who use TxDOT information assets must comply with all the security controls established by agency policies, processes, and procedures; and provide written acknowledgment that they will comply with these standards in the prescribed manner.

Role Specific. Individuals who have operational or statutory responsibility for information, also known as Information Owners, have additional responsibilities, including determining the classification for the data and the protection measures needed.

Information Owners may delegate the day-to-day maintenance of these records to others, including contractors or vendors, as a routine part of their job responsibilities. Those individuals are defined as Information Custodians and also have a distinct set of responsibilities for data classification.

Compliance and Standards

See the “Classify Data Standards” in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Information Protection Policy**.

Section 3 — Encrypt Data

Introduction

TxDOT must protect its data assets from unauthorized and unintended use when the information is being used, in transit, and at rest. Translating data into a secret code to prevent unintended recipients from reading it is commonly refered to as encryption. TxDOT uses encryption to maintain the confidentiality, ensures the integrity, and prevent unauthorized disclosure of its information. This section establishes how encryption is a part of TxDOT's **Information Protection Policy**. It provides a role-based method to address the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

Data that is classified as sensitive or confidential must be encrypted while in-transit and while at-rest. This includes data that is considered internal communications. Encryption at TxDOT, minimally, must meet the National Institute of Standards and Technology (NIST) publication "Federal Information Processing Standards," FIPS 140-2. Additionally TxDOT must meet the following four requirements:

- use cryptography or alternate physical protection
- obtain public key certificates from an approved service provider
- maintain a key management system for their distribution, storage, access, and destruction
- prevent unauthorized and unintended information transfer via shared resources.

General Responsibilities

All Individuals who use TxDOT information assets and are entrusted with sensitive or confidential data must ensure the information is encrypted while in-transit and at-rest.

Information custodians. Information custodians must ensure all sensitive and confidential information is encrypted when it is transmitted, stored, or disposed.

Information owners. Information owners must ensure that sensitive and confidential data is encrypted, and that the keys used are managed and safeguarded.

Information Security Officer (ISO). The ISO is responsible for the protection of systems and communications related to TxDOT's information resources. The ISO must:

- ensure that information owners and custodians and individuals who use information resources comply with the encryption policy for sensitive and confidential data.

- provide the mechanisms to encrypt sensitive and confidential data
- verifies that encryption methods comply with FIPS 140-2 standards

Compliance and Standards

See the “Encrypt Data Standards” in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Information Protection Policy**.

Section 4 — Digital Signatures

Introduction

This section establishes how TxDOT manages the risks of using digital signatures, from their creation through their use, modification, storage, and deletion as part of its **Information Protection Policy**. It provides an individual-based method to address the "Protect" objective of the *Texas CyberSecurity Framework.*

Protocol

TxDOT's processes using digital signatures must encrypt the transactions to be compliant with Federal Information Processing Standards (FIPS). This encryption verifies that the signature belongs to the individual who signed the document and that the document did not change once it was signed. Additionally, it must perform either one of two functions:

- store a record of how the signature was created or
- create a statement proving the document was approved using a digital signature.

General Responsibilities

Individuals who do business with TxDOT electronically, must agree to do so beforehand, show agreement in the digital record, and must not have withdrawn the consent.

Information Security Officer must:

- implement security controls to correctly identify and authenticate individuals
- ensure individuals who use TxDOT information resources comply with the digital signature safeguards issued in the **Information Protection Policy**.

Compliance and Standards

See the "Digital Signatures Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Information Protection Policy**.

Section 5 — Privacy

Introduction

This section discusses how TxDOT safeguards private information as part of its **Information Protection Policy**. Protection begins when private information is collected and remains in effect through the information's life cycle until disposition. This section describes collecting only the minimum, **authorized**, necessary information and provides information for curating a tiered, content-based approach to address the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT administers a Privacy Protection Program to ensure that its employees, business programs, and information systems safeguard the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII). To accomplish this, the Agency must:

- identify the least amount of PII elements relevant to its business processes
- evaluate and review its PII assets regularly
- remove or redact PII in the appropriate, secure manner.

General Responsibilities

All individuals who collect PII on behalf of TxDOT must:

- request the least amount of PII necessary, confirming its accuracy, relevance, timeliness, and completeness
- protect the confidentiality of PII
- provide access to collected PII only to the person it identifies or through legally-binding shared agreements.

Information custodian must:

- ensure PII is used for the authorized purposes only
- remove or redact PII identified as unnecessary
- curate PII to better manage risks.

Information owners must:

- document the legal authority to collect, use, maintain, and share PII
- create process to obtain both tiered and blanket approval from individuals **before** collecting PII

- help individuals understand they are approving or denying TxDOT collection of PII.

Records Management Officer must ensure records that contain PII are maintained securely throughout their lifetime.

Information Security Officer must:

- survey the PII holdings to identify and dispose of information that is no longer necessary
- provide techniques to remove or redact PII
- implement cryptographic mechanisms to prevent unauthorized disclosure and to detect changes to information including:
  - establishing controls for the collection, confidentiality, integrity of PII
  - restricting access to, sharing of, and transmission of PII
  - ensuring proper retention and disposal of PII
  - managing responses to PII security incidents.

Compliance and Standards

See the "Privacy Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Information Protection Policy**.

Section 6 — System and Information Integrity

Introduction

This section describes how TxDOT segregates the many functions of information systems to maintain their quality and integrity. As part of its **Information Protection Policy**, this section requires the separation of systems based on functionality and grants access to a select group of authorized individuals. It provides a holistic approach to address the "Protect" objective of the *Texas CyberSecurity Framework.*

Protocol

TxDOT must provide multiple means of separating access to its information. Commonly referred to as layers of defense, this approach protects the quality and integrity of data assets. Minimally, this includes:

- preventing individuals or systems from accessing a device remotely unless they have the authority to do so and explicitly announced their presence
- using boundary protection devices, such as firewalls, to ensure connections use only approved mechanisms and control the information flow
- terminating network connections when inactivity in session exceeds designated limits
- validating and verifying that the origin of the information matches authenticated individuals and end sources
- separating the functionality within applications to segregate differing levels of permissions, for example: administrative roles, security roles, and user roles. This follows the principle of Least Privilege.

General Responsibilities

Individuals who use Agency information resources must report when they identify any risks, failures, or breaches while performing their duties.

Information Security Officer must:

- provide information owners, custodians, and individuals with necessary information for the safe use of web services and email filtering
- implement security controls for filtering web and email content to prevent data loss
- ensure that information owners and custodians comply with the Internet content filtering boundaries issued in the Intrusion Prevention Policy.

Compliance and Standards

See the "System and Information Integrity Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Information Protection Policy**.

Chapter 5 — Investment Protection

Contents:

Section 1 — Investment Protection Policy

Policy Statement

TxDOT's **Investment Protection Policy** is to safeguard the investment in its infrastructure through a robust and rigorous risk management program that allows business programs to optimize their technology-based processes. The intent of the policy is to have safe, reliable, and optimized infrastructure available to authorized users.

Objectives

The **Investment Protection Policy** has three objectives designed to protect the considerable investment TxDOT has made in its information resources environment. They are:

- assess and manage risks
- protect those who work with information resources
- safeguard software, hardware, system, and environment configurations

Each of these objectives is discussed in the following sections of this chapter. The explanations provide a brief introduction of each objective, list the minimum protocol TxDOT must follow, and assign the responsibility for the work.

Section 2 — Risk Management

Introduction

This section establishes how TxDOT's Risk Management Program protects its investment in information assets through a methodical approach to identify, assess, and reduce risks. It describes the minimum protocol and responsibilities that must be in place to effectively respond to risks and monitor progress. Risk Management provides a cyclical review process to address the "Identify" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT will establish a process of managing risks in a consistent manner. This risk management process will begin during all project development and continue throughout the lifetime of the investment. To accomplish this, it must:

- identify risks
- conduct risk assessments
- document results
- create response plans
- establish ownerships
- monitor response activities.

Requests for exceptions or exemptions from this protocol must originate with the Information Owner and route to the Information Security Officer through the Agency's Exceptions Request Process. The following "*Responsibilities*" discussions provides broad information for any owner seeking an exception to security controls.

Responsibilities

Individuals who use information resources must reduce risks, including:

- identifying all significant known risks
- avoiding unnecessary or unreasonable exposures
- initiating reasonable and appropriate responses.

Information Owners who request exceptions from security controls must provide:

- documented business reasons

- accountability for ensuring TxDOT's investment is protected.

The **Information Security Officer** (ISO) must:

- administer the Risk Management Program
- oversee the Risk Register
- monitor risks responses
- review, then approve or deny exception requests.

Compliance and Standards

See the "Risk Management Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Investment Protection Policy**.

Section 3 — Physical and Personnel Protection

Introduction

This section establishes how TxDOT protects those who work with its information resources as part of its **Investment Protection Policy**. The effort includes adhering to the policies published in the Agency's State Security Policy Manual and the safety controls established in the Occupational Safety Manual. Protecting individuals from evolving threats adds operational rigor to TxDOT's approach to satisfy the "Protect" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT will manage how and when individuals can enter or exit locations where information resources are kept. Typically, this includes obvious controls such as tracking visitors, assigning badges, and ensuring that physical access to secure areas are correctly granted and revoked. In the networked environment, TxDOT will review previously granted privileges to ensure that they change as work assignments and organizational changes occur. Access to physical and networked locations will be a part of TxDOT's on-boarding and Off-boarding Processes.

Secured areas. Access to locations where physical information resources are kept is limited to authorized personnel. (See *TxDOT State Security Policy Manual*, Chapter 1, Section 4) the "Additional precautions include:

- accompanying visitors
- wearing and displaying badges
- logging access to the secure areas
- reviewing access logs
- reporting incidents resulting in a lack of physical security.

Entry points. Entry points are all locations from which access to a physical device or system can be gained. This includes on-site and off-site locations, offices, server rooms, wiring cabinets, etc. All entry points leading to secure areas are controlled and monitored either by security guards or electronic mechanisms. Additional precautions include:

- securing entry points at all times
- monitoring opened doors leading to secured areas
- tracking, securing and verifying keys, combinations, and other physical access devices
- reviewing and maintaining accurate inventory logs
- reporting loss or tampering of security devices.

Preventing damage. Recognizing the environmental conditions that may lead to fires, flooding, and sabotage is the first step toward protecting TxDOT's investment in personnel. Minimal precautions include:

- following the Electrical Safety Program as outlined in the *Occupational Safety Manual*
- using safety equipment properly and as required
- following safety protocols described in user manuals for each device.

Responsibilities

Individuals who use information resources must reduce risks, including:

- following common safety practices when working with electronic equipment
- identifying all significant known risks
- avoiding unnecessary or unreasonable exposures
- initiating reasonable and appropriate responses
- securing mobile devices within a locked shelf or with an approved restraining device
- using a non-interruptible, also known as "uninterruptible," power supply units (UPS) to prevent the loss or fluctuation of electrical power
- securing sensitive or confidential information output
- ensuring output devices only create sensitive or confidential documents when authorized recipient releases it.
- verifying that tools, devices, and software entering the secure areas do not pose a threat to systems.

Information Owners who request exceptions from security controls must provide:

- documented business reasons
- accountability for ensuring TxDOT's investment is protected.

Supervisors must:

- follow hiring procedures in the *Human Resources Policy* manual, Chapter 1
- submit a request whenever employees require higher privileges.

The **Information Security Officer** (ISO) must:

- administer the Risk Management Program
- oversee the Risk Register
- monitor risks responses

- review then approve or deny exception requests
- review and track all individuals who have elevated access privileges.

Compliance and Standards

See the "Physical and Personnel Protection Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Investment Protection Policy**.

Section 4 — Asset Management Protection

Introduction

This section establishes how TxDOT manages its information resources assets as part of its Investment Protection policy, and describes the minimum protocols and responsibilities that must be in place to effectively categorize, inventory, maintain, and decommission both physical (tangible) assets such as hardware, physical documents, facilities, etc. and non-physical (intangible) such as intellectual property, digital records, digital connections, virtual machines, etc. This protocol provides a system-based method to address the "Identify" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT identifies and protects all information resources throughout their life cycle by applying information security principles in the specification, design, development, implementation, and modification of the information system. Each information resource is required to be authorized to operate by the Information Security Officer. This includes:

- determining, documenting, and allocating necessary resources to protect the information systems
- creating a security assessment plan
- maintaining the currency of software and information systems
- testing and evaluating the information system
- certifying the security assessment
- providing testing results and evaluations to the Information Security Office.

General Responsibilities

Individuals who use TxDOT information resources must also maintain and protect them.

Information custodians must maintain accurate inventories of TxDOT's information resources.

Information owners must ensure the information assets within their departments are secure.

Information Security Officer must ensure:

- information owners and custodians adhere to the security standards for asset management
- information resources are properly documented, and

- any assets within the TxDOT environment has an approved authority to operate.

Compliance and Standards

See the "Asset Management Protection Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Investment Protection Policy**.

Chapter 6 — Business Continuity

Contents:

Section 1 — Business Continuity Policy

The **Business Continuity Policy** is to create, test, and maintain a system of high-level implementation plans for restoring critical information systems to the latest documented functionality. The intent of the policy is to ensure that TxDOT can resume its services after a natural or man-made incident prohibits the Agency from accessing its virtual or physical information resources.

Objectives

Four objectives serve as the cornerstones to ensure TxDOT's information assets can be redeployed to support its business services:

- managing change
- creating contingencies
- responding to incidents
- recovering from disasters.

Each of these objectives is discussed in the following sections of this chapter. Each outline provides a brief introduction of the objective, lists the minimum protocol TxDOT must follow, and assigns the responsibility for the work.

Section 2 — Change Management

Introduction

This section establishes how TxDOT uses configuration, change, and patch management processes as part of its Business Continuity policy, and describes the minimum standards that must be in place to effectively support continued business functions when normal operations have been compromised. This approach addresses the "Recover" objective of the *Texas CyberSecurity Framework* and provides a baseline for business functions.

Protocol

TxDOT will create an Authority to Operate (ATO) certification process during which the Information Security Office reviews system security configurations. Documentation gathered during this process will become the baseline from which all changes are measured. The baseline for each information system will be reviewed and updated whenever there is a change in configuration. TxDOT must maintain at least N-1 currency for all its software assets.

All changes to the baseline configuration must be evaluated, approved, tested, released, and documented. TxDOT approves changes in three approaches through the Change Approval Board (CAB): regular changes, normal changes, and emergency changes. Changes will not be released into production without the approval of the ISO and the system or information owner. Additionally, changes will be audited against the ATO configuration at planned intervals.

Patch management follows the Change Management processes. TxDOT uses software, firmware, or middleware only from vendors who provide continued support and updates. These vendors provide updates and service packs; TxDOT obtains and tracks information on these updates on a regular basis depending on each vendor's release schedule.

General Responsibilities

Individuals who use TxDOT information resources andwho need to request changes to an information system will follow the change request procedures. All information owners will ensure that their systems are updated and patched to ensure information systems are in compliance with this policy.

The Information Security Office must:

- review proposed configurations
- grant Authority to Operate certificates.

Compliance and Standards

See the "Change Management Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Business Continuity Policy**.

Section 3 — Contingency Planning

Introduction

This section establishes how TxDOT uses interim measures to recover information resources after a disruption. It describes the minimum standards that must be in place to effectively create a plan for how to respond if routine business operations are suspended. Contingency planning provides a system-based method to address the "Recover" objective of the *Texas CyberSecurity Framework*.

Protocol

TxDOT will ensure that its information systems have contingency plans to address its backups, disaster recovery, and emergency mode operations. Contingency plans must be tested and reviewed yearly. They must include the periodic testing of backup media to verify its readability. Plans must ensure each system has enough backup data available to restore the systems to a recent, operable, and accurate state. See NIST Special Publication 800-34 revision 1, "*Contingency Planning Guide for Federal Information Systems*" for steps in creating a contingency plan.

General Responsibilities

Information custodians assist the information owners in ensuring the contingency planning policy is followed by maintaining and testing the backups and contingency plans.

Information owners are responsible for developing, testing, reviewing, and maintaining contingency plans for all of their corresponding information systems.

Information Security Officer is responsible for reviewing the contingency plans in coordination with the information owners and information custodians.

Compliance and Standards

See the "Contingency Planning Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Business Continuity Policy**.

Section 4 — Incident Response

Introduction

This section establishes how TxDOT maintains an Incident Response Plan in order to properly respond to, document, and track incidents. The Incident Response Plan provides a high-level approach for TxDOT's response when information security policies are breached. It provides an emergency-based method to address the "Response" objective of the *Texas CyberSecurity Framework*.

CAUTION: Documents related to incident response are confidential. The incident response plan needs will be distributed to department heads and other stake holders on a need-to-know basis.

Protocol

An incident response plan must describe a strategic response to a breach of routine business practices and provide sufficient details to continue business functions. The plan is tested annually and is updated as needed. TxDOT's response includes assembling a trained incident response team.

All incidents are reported to TxDOT's Information Security Officer (ISO) as soon as they are discovered. The ISO notifies stakeholders according to the escalation levels established in the incident response plan. TxDOT implements an automated incident handling response to include the preparation, detection and analysis, containment, eradication, and recovery from incidents.

WARNING: Information about security incidents will be on a "need-to-know" basis and are confidential in nature. Reports are reviewed and approved by the Information Security Officer (ISO) prior to release to outside agencies.

General Responsibilities

Information Custodians assist the incident response teams with their incident investigations.

Information Owners review, test, and update the incident response plan in coordination with the Information Security Officer.

Information Security Officer must:

- oversee the establishment and training of the incident response teams.
- review and test updates to the incident response plans are aligned with current standards.
- ensure that updates to the incident response plans are aligned with current standards.

Compliance and Standards

See the "Incident Response Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Business Continuity Policy**.

Section 5 — Disaster Recovery

Introduction

TxDOT must plan how to recover and support the continuity of services if a disruption denies access to a primary operations facility. The sole objective of this plan is to re-deploy affected services at a designated alternate site. This objective addresses the "Recover" objective of the *Texas CyberSecurity Framework.*

Protocol

A disaster recovery plan is a site-specific plan of action to direct TxDOT in enabling its services when access to the daily operational location is prohibited. Document the disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works. The plan must include a strategy to ensure all critical information is backed up and can be deployed at alternate sites.

Each plan must include:

- identified software applications and their data
- assigned priority for hardware and software restoration
- specified procedures for obtaining necessary equipment
- Written instructions to recreate an operational environment for supporting the systems.

Alternate Sites. Alternate sites must be located sufficiently apart to prevent one disaster from affecting multiple facilities. The sites are designated either hot, warm, or cold based on the amount of time necessary to make the services available. Three system attributes will determine which alternative site a system will use:

- How critical is the system?
- How long is the recovery time for the system?
- What are the effects of a system outage?

General Responsibilities

Planning for continued service after a disaster is the responsibility of all stakeholders who have a duty to provide that service. Planning is a coordinated effort that requires the input from the individuals, information custodians, information owners, department heads, the information security officer, and the head of the agency.

Compliance and Standards

See the "Disaster Recovery Standards" in the *Information Security Standards* manual for a list of the minimum standards necessary to comply with this objective of the **Business Continuity Policy**.