Security Control Standards Catalog

Texas Department of Information Resources

Version 2.0

Effective Date: January 20, 2022

Table of Contents

OVERVIEW

PURPOSE

The purpose of the Security Control Standards Catalog (catalog) is to provide Texas state agencies and institutions of higher education (subsequently referred to as *state agencies*) with specific guidance for implementing security controls in a format that easily aligns with the **National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST 800-53 Revision 5)**.

Terms and definitions in this catalog are based on NIST, unless otherwise defined by Texas state statute, rules, or guidelines. For questions concerning terms or definitions, contact DIR Security email.

APPLICATION OF MORE STRINGENT STANDARDS

This catalog specifies the minimum baselines for required information security controls for all State of Texas agencies and their information resources. Controls in this catalog are not exclusively technical in nature and therefore their application is not inherently limited to information systems.

Each state agency should select and apply any additional security controls, control baselines, or control enhancements for information resources or scenarios where an elevated security posture is required to mitigate risks identified by the agency.

For systems that store, process, or transmit confidential and/or information subject to other security regulatory requirements, additional security controls or control baselines should be selected and applied commensurate with the level of risk and confidentiality, integrity, and availability requirements of the system.

The agency head may employ standards for the cost-effective information security of information and information resources within or under the supervision of that state agency that are more stringent than the standards the department prescribes within this catalog if the more stringent standards:

(1) contain at least the applicable standards issued by the department; or

(2) are consistent with applicable federal law, policies and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the agency.

For more information related to information security requirements for state agencies, refer to **1 Texas Administrative Code Chapter 202**, concerning Information Security Standards.

DOCUMENT LIFECYCLE

DIR works with representatives from state agencies to review and develop the controls necessary to maintain reasonable security measures to protect state resources.

Prior to publishing new or revised standards, DIR will solicit comments on new controls from Information Resources Managers and Information Security Officers of state agencies.

REVISION HISTORY

Version	Date	Change Description
0.1	3/23/2014	Released Draft Version 0.1
1.0	10/22/2014	Released Draft Version 1.0
1.1	3/17/2015	Released Final Version 1.0
1.2	4/3/2015	Corrected date on cover; added missing legacy TAC referenced in Appendix A; ensured pdf is fully searchable
1.3	2/26/2016	Modified or corrected examples for AC-23, AC-24, AC-25, AR-5, CM-8, PM-7; corrected TAC 202 reference in PL-1, SC-13; Added Program Management Controls to Appendix A
2.0	1/20/2022	DIR Board approval of Version 2.0. Control language updated to align with NIST SP 800-53 Revision 5; Introduction of New SR control family.

RISK EXCEPTIONS

Any exception to the following controls shall be approved, justified, and documented in accordance with 1 Texas Administrative Code Chapter 202.

PRIVACY CONTROLS

While NIST 800-53 Revision 5 took substantial steps to integrate security and privacy requirements, this catalog has not adopted privacy-specific control families. Security-focused controls may include privacy-related components, but the defined privacy control families are not included within this catalog. State agencies should work with the employees or divisions responsible for privacy-related requirements to determine the appropriate privacy activities and controls for the needs of their state agency.

For more information on the NIST SP 800-53 Privacy Baseline and Controls, refer to https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&privacy_baseline=Yes

REQUIRED IMPLEMENTATION DATES

Each control in this catalog contains a required by date that indicates when the control must be implemented by each agency. Required by dates were selected based on the following characteristics of the control changes.

New Controls

Controls that were not required in the previous iteration of the DIR Control Standards Catalog that have been adopted in this revision are required to be in place no later than 18 months after the adoption of this catalog.

Existing Controls with More than Administrative Changes

Controls that were required in the previous iteration of the DIR Control Standards Catalog that have been updated with more than editorial/administrative changes (i.e. require additional or modified implementation activities) are required to be in place no later than 18 months after the adoption of this catalog.

Existing Controls with Administrative or Nonsubstantial Changes

Controls that were required in the previous iteration of the DIR Control Standards Catalog that have been updated with nonsubstantial revisions are required to be in place no later than 12 months after the adoption of this catalog.

NUMBER OF CONTROLS BY FAMILY

ID	Control Family	Number of Controls/ Enhancements
AC	Access Control	13
AT	Awareness and Training	4
AU	Accountability, Audit, and Risk Management	10
CA	Security Assessment and Authorization	9
CM	Configuration Management	9
CP	Contingency Planning	8
IA	Identification and Authentication	10
IR	Incident Response	9
MA	Maintenance	4
MP	Media Protection	4
PE	Physical and Environmental Protection	11
PL	Planning	3
PM	Program Management	12
PS	Personnel Security	8
RA	Risk Assessment	6
SA	System and Service Acquisition	10
SC	System and Communication Protection	11
SI	System and Information Integrity	7
SR	Supply Chain Risk Management	6
	Total	**154**

CONTROL DETAILS AND SAMPLE FORMAT

Each control group is organized under its group identification code and title, *e.g.,* **AC – ACCESS CONTROL**

Information about each control is presented in the following format.

[Control ID] [Control Name]

NIST BASELINE: This is the NIST baseline associated with the respective control. This is an informational field only. The DIR Security Control Standards Catalog does not contain distinct baselines. As such, agencies should determine whether additional controls or control baselines are appropriate for a given information system.

PRIVACY BASELINE: This field indicates whether the control is part of the NIST 800-53 Revision 5 Privacy Baseline. This is an informational field only.

NEW REQUIREMENT: This field indicates whether the control is a new requirement of the DIR Security Control Standards Catalog.

REQUIRED BY: This field indicates the date by which the control must be in place by the agency. Agencies shall maintain compliance with the prior version of the control standards catalog until the control description indicated in this catalog has been implemented.

STATE IMPLEMENTATION DETAILS: This field provides Texas-specific guidance or additional requirements that apply to the control and must be incorporated into the implementation of the control.

AC – ACCESS CONTROL

AC-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

AC-2 | ACCOUNT MANAGEMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Define and document the types of accounts allowed for use within the system;

b. Assign account managers;

c. Establish conditions for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, and conditions];

g. Monitor the use of accounts;

h. Notify account managers and [Assignment: organization-defined personnel or roles] within:

1. [Assignment: organization-defined time-period] when accounts are no longer required;

2. [Assignment: organization-defined time-period] when users are terminated or transferred; and

3. [Assignment: organization-defined time-period] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. [Assignment: organization-defined attributes (as required)];

j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];

k. Establish and implement a process for changing shared or group account credentials (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

STATE IMPLEMENTATION DETAILS

Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from or shared between one state agency to another or from or between a state agency to a contractor or other third party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum.

AC-3 | ACCESS ENFORCEMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

STATE IMPLEMENTATION DETAILS

1. Access to state information resources shall be appropriately managed.

2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

AC-5 | SEPARATION OF DUTIES

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and

b. Define system access authorizations to support separation of duties.

STATE IMPLEMENTATION DETAILS

N/A

AC-6 | LEAST PRIVILEGE

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

STATE IMPLEMENTATION DETAILS

N/A

AC-7 | UNSUCCESSFUL LOGON ATTEMPTS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time-period]; and

b. Automatically [Selection (one or more)]: lock the account or node for an [Assignment: organization-defined time-period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action] when the maximum number of unsuccessful attempts is exceeded.

STATE IMPLEMENTATION DETAILS

1. As technology permits, state agencies should enforce account lockouts after, at minimum, 10 failed attempts. This threshold may be lowered for Moderate or High risk systems.

2. Accounts locked out due to multiple incorrect logon attempts should stay locked out for a minimum of 15 minutes. Accounts for Moderate or High risk systems should remain locked until reset by an administrator.

AC-8 | SYSTEM USE NOTIFICATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government or State of Texas Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information [Assignment: organization-defined conditions] before granting further access to the publicly accessible system;

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

STATE IMPLEMENTATION DETAILS

System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:

- Unauthorized use is prohibited;
- Usage may be subject to security testing and monitoring;
- Misuse is subject to criminal prosecution; and
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

AC-14 | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

STATE IMPLEMENTATION DETAILS

N/A

AC-17 | REMOTE ACCESS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

STATE IMPLEMENTATION DETAILS

N/A

AC-18 | WIRELESS ACCESS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

STATE IMPLEMENTATION DETAILS

State agencies shall establish the requirements and security restrictions for installing or providing access to the state agency's information resources systems. The wireless policy shall address the following topic areas:

1. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID.

2. Transmitting and Encrypting Information. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information.

State agencies shall not transmit confidential information via a wireless connection to or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards as detailed within this Security Control Standards Catalog, are used to protect the information.

3. Installation or Use of Wireless Personal Area Networks. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state agency IT systems by individuals without the approval of the state agency information resources manager.

AC-19 | ACCESS CONTROL FOR MOBILE DEVICES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

STATE IMPLEMENTATION DETAILS

N/A

AC-20 | USE OF EXTERNAL SYSTEMS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Establish [Selection (one or more)]: [Assignment: organization-defined terms and conditions]; [Assignment: organization-defined controls asserted to be implemented on external systems], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

a. Access the system from external systems; and

b. Process, store, or transmit organization-controlled information using external systems.

STATE IMPLEMENTATION DETAILS

N/A

AC-22 | PUBLICLY ACCESSIBLE CONTENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.

STATE IMPLEMENTATION DETAILS

N/A

AT – AWARENESS AND TRAINING

AT-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more)]: organization-level; mission/business process-level; system-level] awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

Security awareness training shall be delivered in accordance with Texas Government Code § 2054.519.

AT-2 | AWARENESS TRAINING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Provide security and privacy awareness training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and

2. When required by system changes; and

b. Update awareness training [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

Security awareness training shall be delivered in accordance with Texas Government Code § 2054.519.

AT-3 | ROLE-BASED TRAINING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:

1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and

2. When required by system changes; and

b. Update role-based training [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

Security awareness training shall be delivered in accordance with Texas Government Code § 2054.519.

AT-4 | TRAINING RECORDS

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [Assignment: organization-defined time-period].

STATE IMPLEMENTATION DETAILS

Security awareness training shall be delivered in accordance with Texas Government Code § 2054.519.

AU – ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

AU-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more)]: organization-level; mission/business process-level; system-level] audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

AU-2 | EVENT LOGGING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2 a.) along with the frequency of (or situation requiring) logging for each identified event type];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation or modification of, or affect the release of confidential information.

Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software, and for all changes to automated security or access rules.

Based upon astate agency’s assessment of the risk, the state agency shall maintain a sufficiently complete history of transactions to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.

AU-3 | CONTENT OF AUDIT RECORDS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

STATE IMPLEMENTATION DETAILS

N/A

AU-4 | AUDIT LOG STORAGE CAPACITY

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

STATE IMPLEMENTATION DETAILS

N/A

AU-5 | RESPONSE TO AUDIT LOGGING PROCESS FAILURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period] in the event of an audit logging process failure; and

b. Take the following additional actions: [Assignment: organization-defined additional actions].

STATE IMPLEMENTATION DETAILS

N/A

AU-6 | AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity];

b. Report findings to [Assignment: organization-defined personnel or roles]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

STATE IMPLEMENTATION DETAILS

N/A

AU-8 | TIME STAMPS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

STATE IMPLEMENTATION DETAILS

N/A

AU-9 | PROTECTION OF AUDIT INFORMATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

STATE IMPLEMENTATION DETAILS

N/A

AU-11 | AUDIT RECORD RETENTION

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Retain audit records for [Assignment: organization-defined time-period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

STATE IMPLEMENTATION DETAILS

N/A

AU-12 | AUDIT RECORD GENERATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];

b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

STATE IMPLEMENTATION DETAILS

N/A

CA – SECURITY ASSESSMENT AND AUTHORIZATION

CA-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CA-2 | CONTROL ASSESSMENTS

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;
2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

c. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

d. Produce a control assessment report that document the results of the assessment; and

e. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].

STATE IMPLEMENTATION DETAILS

A review of the agency's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the agency head or his or her designated representative(s).

CA-3 | INFORMATION EXCHANGE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more)]: interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement];

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CA-5 | PLAN OF ACTION AND MILESTONES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, audits, and continuous monitoring activities.

STATE IMPLEMENTATION DETAILS

N/A

CA-6 | AUTHORIZATION

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CA-7 | CONTINUOUS MONITORING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];

b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CA-7 (4) CONTINUOUS MONITORING | RISK MONITORING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

STATE IMPLEMENTATION DETAILS

N/A

CA-8 | PENETRATION TESTING

NIST BASELINE: High

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

STATE IMPLEMENTATION DETAILS

Texas Government Code § 2054.516(a)(2) requires each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information to subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

CA-9 | INTERNAL SYSTEM CONNECTIONS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [Assignment: organization-defined conditions]; and

d. Review [Assignment: organization-defined frequency] the continued need for each internal connection.

STATE IMPLEMENTATION DETAILS

N/A

CM – CONFIGURATION MANAGEMENT

CM-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CM-2 | BASELINE CONFIGURATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [Assignment: organization-defined frequency];

2. When required due to [Assignment: Assignment organization-defined circumstances]; and

3. When system components are installed or upgraded.

STATE IMPLEMENTATION DETAILS

N/A

CM-4 | IMPACT ANALYSES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

STATE IMPLEMENTATION DETAILS

All security-related information resources changes shall be approved by the information owner through a change control process.

Approval shall occur prior to implementation by the state agency or independent contractors.

CM-5 | ACCESS RESTRICTIONS FOR CHANGE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

STATE IMPLEMENTATION DETAILS

N/A

CM-6 | CONFIGURATION SETTINGS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

STATE IMPLEMENTATION DETAILS

N/A

CM-7 | LEAST FUNCTIONALITY

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, software, and/or services].

STATE IMPLEMENTATION DETAILS

N/A

CM-8 | SYSTEM COMPONENT INVENTORY

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Is at the level of granularity deemed necessary for tracking and reporting; and

4. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CM-10 | SOFTWARE USAGE RESTRICTIONS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

STATE IMPLEMENTATION DETAILS

N/A

CM-11 | USER-INSTALLED SOFTWARE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Establish [Assignment: organization-defined policies] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and

c. Monitor policy compliance [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

CP – CONTINGENCY PLANNING

CP-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] contingency planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

State agencies shall maintain written Continuity of Operations Plans in compliance with Texas Labor Code § 412.054 that address information resources so that the effects of a disaster will be minimized and the state agency will be able either to maintain or quickly resume mission-critical functions.

CP-2 | CONTINGENCY PLAN

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop a contingency plan for the system that:

1. Identifies essential missions and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;

5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; and

6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [Assignment: organization-defined frequency];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and

g. Protect the contingency plan from unauthorized disclosure and modification.

STATE IMPLEMENTATION DETAILS

The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:

1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:

A. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

B. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

2. Disruption impacts and allowable outage times to include:

A. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.

B. Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:

A. Preventative controls and processes such as backup power, excess capacity, environmental sensors and alarms.

B. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.

d. Disaster Recovery Plan--Each state agency shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

2. Identify recovery resources and a source for each;

3. Contain step-by-step implementation instructions;

4. Include provisions for annual testing.

CP-3 | CONTINGENCY TRAINING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Provide contingency training to system users consistent with assigned roles and responsibilities:

a. Within [Assignment: organization-defined time-period] of assuming a contingency role or responsibility;

b. When required by system changes; and

c. [Assignment: organization-defined frequency] thereafter.

STATE IMPLEMENTATION DETAILS

N/A

CP-4 | CONTINGENCY PLAN TESTING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

STATE IMPLEMENTATION DETAILS

Each state agency's written disaster recovery plan shall include provisions for annual testing.

CP-6 | ALTERNATE STORAGE SITE

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

STATE IMPLEMENTATION DETAILS

Mission-critical information shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized state agency representatives.

CP-9 | SYSTEM BACKUP

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

c. Conduct backups of system documentation, including security and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and

d. Protect the confidentiality, integrity, and availability of backup information.

STATE IMPLEMENTATION DETAILS

N/A

CP-10 | SYSTEM RECOVERY AND RECONSTITUTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time-period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

STATE IMPLEMENTATION DETAILS

N/A

CP-11 | ALTERNATE COMMUNICATIONS PROTOCOLS

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

STATE IMPLEMENTATION DETAILS

N/A

IA – IDENTIFICATION AND AUTHENTICATION

IA-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

STATE IMPLEMENTATION DETAILS

Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

IA-2 (1) | MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Implement multifactor authentication for access to privileged accounts for [organization-defined information systems or system categorizations].

STATE IMPLEMENTATION DETAILS

N/A

IA-2 (2) | MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Implement multifactor authentication for access to non-privileged accounts for selection [organization-defined systems; organization-defined system categorizations].

STATE IMPLEMENTATION DETAILS

N/A

IA-4 | IDENTIFIER MANAGEMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Manage system identifiers by:

a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [Assignment: organization-defined time-period].

STATE IMPLEMENTATION DETAILS

A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state agency change.

IA-5 | AUTHENTICATOR MANAGEMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

f. Changing default authenticators prior to first use;

g. Changing or refreshing authenticators [Assignment: organization-defined time-period by authenticator type];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

j. Changing authenticators for group or role accounts when membership to those accounts changes.

STATE IMPLEMENTATION DETAILS

N/A

IA-6 | AUTHENTICATOR FEEDBACK

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

STATE IMPLEMENTATION DETAILS

N/A

IA-7 | CRYPTOGRAPHIC MODULE AUTHENTICATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

STATE IMPLEMENTATION DETAILS

N/A

IA-8 | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

STATE IMPLEMENTATION DETAILS

N/A

IA-11 | RE-AUTHENTICATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

STATE IMPLEMENTATION DETAILS

N/A

IR – INCIDENT RESPONSE

IR-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

State agencies shall assess the significance of a security incident based upon the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks.

IR-2 | INCIDENT RESPONSE TRAINING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Provide incident response training to system users consistent with assigned roles and responsibilities:

a. Within [Assignment: organization-defined time-period] of assuming an incident response role or responsibility or acquiring system access;

b. When required by system changes; and

c. [Assignment: organization-defined frequency] thereafter.

STATE IMPLEMENTATION DETAILS

The state agency trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.

IR-3 | INCIDENT RESPONSE TESTING

NIST BASELINE: Moderate

PRIVACY BASELINE: Yes

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].

STATE IMPLEMENTATION DETAILS

N/A

IR-4 | INCIDENT HANDLING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

STATE IMPLEMENTATION DETAILS

N/A

IR-5 | INCIDENT MONITORING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Track and document security, privacy, and supply chain incidents.

STATE IMPLEMENTATION DETAILS

N/A

IR-6 | INCIDENT REPORTING

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Require personnel to report suspected security, privacy, and supply chain incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and

b. Report security, privacy, and supply chain incident information to [Assignment: organization-defined authorities].

STATE IMPLEMENTATION DETAILS

Reporting of security incidents and the investigation and restoration of operations following a security incident assessed to involve suspected criminal activity shall comply with 1 Texas Administrative Code § 202.23(b).

IR-7 | INCIDENT RESPONSE ASSISTANCE

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of security, privacy, and supply chain incidents.

STATE IMPLEMENTATION DETAILS

The state agency provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability.

IR-8 | INCIDENT RESPONSE PLAN

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and
9. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and

e. Protect the incident response plan from unauthorized disclosure and modification.

STATE IMPLEMENTATION DETAILS

N/A

IR-9 | INFORMATION SPILLAGE RESPONSE

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Respond to information spills by:

a. Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: [Assignment: organization-defined actions].

STATE IMPLEMENTATION DETAILS

N/A

MA – MAINTENANCE

MA-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

MA-2 | CONTROLLED MAINTENANCE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].

STATE IMPLEMENTATION DETAILS

N/A

MA-4 | NONLOCAL MAINTENANCE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

STATE IMPLEMENTATION DETAILS

N/A

MA-5 | MAINTENANCE PERSONNEL

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

STATE IMPLEMENTATION DETAILS

N/A

MP – MEDIA PROTECTION

MP-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] media protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

MP-2 | MEDIA ACCESS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

STATE IMPLEMENTATION DETAILS

N/A

MP-6 | MEDIA SANITIZATION

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

STATE IMPLEMENTATION DETAILS

Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, state agencies shall assess whether to remove data from any associated storage device.

Electronic state records shall be destroyed in accordance with Texas Government Code § 441.185 and in compliance with the state agency's records retention schedule. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the state agency shall retain a hard copy or other electronic copy of the record for the required retention period.

If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are provided in the "Sale or Transfer of Computers and Software" guidelines available at https://dir.texas.gov/resource-library-item/sale-or-transfer-computers-and-software.

State agencies shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:

- date;
- description of the item(s) and serial number(s);
- inventory number(s);
- the process and sanitization tools used to remove the data or method of destruction; and
- the name and address of the organization the equipment was transferred to.

MP-7 | MEDIA USE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

STATE IMPLEMENTATION DETAILS

N/A

PE – PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more)]: organization-level; mission/business process-level; system-level] physical and environmental protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

PE-2 | PHYSICAL ACCESS AUTHORIZATIONS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and

d. Remove individuals from the facility access list when access is no longer required.

STATE IMPLEMENTATION DETAILS

N/A

PE-3 | PHYSICAL ACCESS CONTROL

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using [Selection (one or more)]:

[Assignment: organization-defined physical access control systems or devicesor guards];

b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined controls];

d. Escort visitors and monitor visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and

g. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

STATE IMPLEMENTATION DETAILS

N/A

PE-6 | MONITORING PHYSICAL ACCESS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

STATE IMPLEMENTATION DETAILS

N/A

PE-8 | VISITOR ACCESS RECORDS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time-period];

b. Review visitor access records [Assignment: organization-defined frequency]; and

c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

STATE IMPLEMENTATION DETAILS

N/A

PE-12 | EMERGENCY LIGHTING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

STATE IMPLEMENTATION DETAILS

N/A

PE-13 | FIRE PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

STATE IMPLEMENTATION DETAILS

Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

PE-14 | ENVIRONMENTAL CONTROLS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Maintain [Selection (one or more)]: temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and

b. Monitor environmental control levels [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

PE-15 | WATER DAMAGE PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

STATE IMPLEMENTATION DETAILS

N/A

PE-16 | DELIVERY AND REMOVAL

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and

b. Maintain records of the system components.

STATE IMPLEMENTATION DETAILS

N/A

PE-17 | ALTERNATE WORK SITE

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;

b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

STATE IMPLEMENTATION DETAILS

N/A

PL – PLANNING

PL-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more)]: organization-level; mission/business process-level; system-level] planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

The state agency information security officer reports annually on state agency information security program in compliance with 1 Texas Administrative Code §§ 202.23(a), 202.73(a).

PL-2 | SYSTEM SECURITY AND PRIVACY PLANS

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operational context of the system in terms of missions and business processes;

4. Provide the security categorization of the system, including supporting rationale;

5. Describe any specific threats to the system that are of concern to the organization;

6. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

7. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

8. Provide an overview of the security and privacy requirements for the system;

9. Identify any relevant control baselines or overlays, if applicable;

10. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

11. Include risk determinations for security and privacy architecture and design decisions;

12. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and

13. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];

c. Review the plans [Assignment: organization-defined frequency];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

STATE IMPLEMENTATION DETAILS

N/A

PL-4 | RULES OF BEHAVIOR

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more)]: [Assignment: organization-defined frequency]; [when the rules are revised or updated].

STATE IMPLEMENTATION DETAILS

N/A

PM – PROGRAM MANAGEMENT

PM-1 | INFORMATION SECURITY PROGRAM PLAN

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop and disseminate an organization-wide information security program plan that:

1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

3. Reflects the coordination among organizational entities responsible for information security; and

4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Review the organization-wide information security program plan [Assignment: organization-defined frequency];

c. Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and

d. Protect the information security program plan from unauthorized disclosure and modification.

STATE IMPLEMENTATION DETAILS

N/A

PM-2 | INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

STATE IMPLEMENTATION DETAILS

The Information Security Officer is charged with the responsibilities enumerated at Texas Government Code § 2054.136 and 1 Texas Administrative Code § 202.21.

PM-3 | INFORMATION SECURITY AND PRIVACY RESOURCES

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;

b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and

c. Make available for expenditure, the planned information security and privacy resources.

STATE IMPLEMENTATION DETAILS

N/A

PM-4 | PLAN OF ACTION AND MILESTONES PROCESS

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Implement a process to ensure that plans of action and milestones for the information security and privacy programs and associated organizational systems:

1. Are developed and maintained;

2. Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, the State of Texas, and the Nation; and

3. Are reported in accordance with established reporting requirements.

b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

STATE IMPLEMENTATION DETAILS

N/A

PM-5 | SYSTEM INVENTORY

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.

STATE IMPLEMENTATION DETAILS

N/A

PM-6 | MEASURES OF PERFORMANCE

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Develop, monitor, and report on the results of information security and privacy measures of performance.

STATE IMPLEMENTATION DETAILS

N/A

PM-7 | ENTERPRISE ARCHITECTURE

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, the State of Texas, and the Nation.

STATE IMPLEMENTATION DETAILS

N/A

PM-9 | RISK MANAGEMENT STRATEGY

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develops a comprehensive strategy to manage:

1. Security risk to organizational operations and assets, individuals, other organizations, the State of Texas, and the Nation associated with the operation and use of organizational systems; and

2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement the risk management strategy consistently across the organization; and

c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

STATE IMPLEMENTATION DETAILS

N/A

PM-10 | AUTHORIZATION PROCESS

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Integrate the authorization processes into an organization-wide risk management program.

STATE IMPLEMENTATION DETAILS

N/A

PM-14 | TESTING, TRAINING, AND MONITORING

NIST BASELINE: None

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:

1. Are developed and maintained; and

2. Continue to be executed; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

STATE IMPLEMENTATION DETAILS

N/A

PM-15 | SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

a. To facilitate ongoing security and privacy education and training for organizational personnel;

b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. To share current security and privacy information, including threats, vulnerabilities, and incidents.

STATE IMPLEMENTATION DETAILS

N/A

PM-16 | THREAT AWARENESS PROGRAM

NIST BASELINE: None

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

STATE IMPLEMENTATION DETAILS

N/A

PS – PERSONNEL SECURITY

PS-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] personnel security policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

PS-2 | POSITION RISK DESIGNATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

All authorized users (including, but not limited to, state agency personnel, temporary employees, and employees of independent contractors) of the state agency's information resources shall formally acknowledge that they will comply with the security policies and procedures of the state agency or they shall not be granted access to information resources. The state agency head or their designated representative will determine the method of acknowledgement and how often this acknowledgement must be reexecuted by the user to maintain access to state agency information resources.

PS-3 | PERSONNEL SCREENING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].

STATE IMPLEMENTATION DETAILS

N/A

PS-4 | PERSONNEL TERMINATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Upon termination of individual employment:

a. Disable system access within [Assignment: organization-defined time-period];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

STATE IMPLEMENTATION DETAILS

N/A

PS-5 | PERSONNEL TRANSFER

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time-period following the formal transfer action];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period].

STATE IMPLEMENTATION DETAILS

N/A

PS-6 | ACCESS AGREEMENTS

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [Assignment: organization-defined frequency]; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

PS-7 | EXTERNAL PERSONNEL SECURITY

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time-period]; and

e. Monitor provider compliance with personnel security requirements.

STATE IMPLEMENTATION DETAILS

N/A

PS-8 | PERSONNEL SANCTIONS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

STATE IMPLEMENTATION DETAILS

N/A

RA – RISK ASSESSMENT

RA-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

RA-2 | SECURITY CATEGORIZATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

STATE IMPLEMENTATION DETAILS

State agencies are responsible for identifying and defining all information classification categories except the Confidential Information category, as defined by 1 Texas Administrative Code Chapter 202, Subchapter A, and establishing the appropriate controls for each.

RA-3 | RISK ASSESSMENT

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Conduct a risk assessment, including:

1. The likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

2. The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];

d. Review risk assessment results [Assignment: organization-defined frequency];

e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

STATE IMPLEMENTATION DETAILS

The state agency shall perform and document risk assessments and make and document risk management decisions in compliance with 1 Texas Administrative Code §§ 202.25, 202.27. A state agency's security risk management plan may be excepted from disclosure under Texas Government Code § 2054.077(c) or Texas Government Code § 552.139.

RA-3 (1) | SUPPLY CHAIN RISK ASSESSMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

(a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and

(b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

STATE IMPLEMENTATION DETAILS

N/A

RA-5 | VULNERABILITY MONITORING AND SCANNING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

STATE IMPLEMENTATION DETAILS

The state agency scans for vulnerabilities in the information system at least annually or when significant new vulnerabilities potentially affecting the system are identified and reported.

RA-7 | RISK RESPONSE

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

STATE IMPLEMENTATION DETAILS

N/A

SA – SYSTEM AND SERVICE ACQUISITION

SA-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and services acquisition policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

SA-2 | ALLOCATION OF RESOURCES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

STATE IMPLEMENTATION DETAILS

N/A

SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

STATE IMPLEMENTATION DETAILS

A state agency shall include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

SA-4 | ACQUISITION PROCESS

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

STATE IMPLEMENTATION DETAILS

N/A

SA-5 | SYSTEM DOCUMENTATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Obtain administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;

d. Protect documentation as required, in accordance with the organizational risk management strategy; and

e. Distribute documentation to [Assignment: organization-defined personnel or roles].

STATE IMPLEMENTATION DETAILS

N/A

SA-8 | SECURITY AND PRIVACY ENGINEERING PRINCIPLES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

STATE IMPLEMENTATION DETAILS

N/A

SA-9 | EXTERNAL SYSTEM SERVICES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].

STATE IMPLEMENTATION DETAILS

N/A

SA-10 | DEVELOPER CONFIGURATION MANAGEMENT

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];

b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

STATE IMPLEMENTATION DETAILS

The information owner shall approve all security-related information resources changes through a change control process. Approval shall occur prior to implementation by the state agency or independent contractors.

SA-11 | DEVELOPER TESTING AND EVALUATION

NIST BASELINE: Moderate

PRIVACY BASELINE: Yes

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy assessments;

b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

STATE IMPLEMENTATION DETAILS

N/A

SA-22 | UNSUPPORTED SYSTEM COMPONENTS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].

STATE IMPLEMENTATION DETAILS

N/A

SC – SYSTEM AND COMMUNICATION PROTECTION

SC-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

SC-5 | DENIAL OF SERVICE PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. [Selection: protect against; limit] the effects of the following types of denial of service events: [Assignment: organization-defined types of denial of service events]; and

b. Employ the following controls to achieve the denial of service objective: [Assignment: organization-defined controls by type of denial of service event].

STATE IMPLEMENTATION DETAILS

N/A

SC-7 | BOUNDARY PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Monitor and control communications at the external interfaces to the system and at key internal interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

STATE IMPLEMENTATION DETAILS

N/A

SC-8 | TRANSMISSION CONFIDENTIALITY AND INTEGRITY

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.

STATE IMPLEMENTATION DETAILS

Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted with, at minimum, a 128-bit encryption algorithm. A state agency may also choose to implement encryption for other data classifications.

SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

STATE IMPLEMENTATION DETAILS

N/A

SC-13 | CRYPTOGRAPHIC PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Determine the [Assignment: organization-defined cryptographic uses]; and

b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].

STATE IMPLEMENTATION DETAILS

Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented state agency risk management decisions.

Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted as described by SC-8.

Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.

Storing confidential information on portable devices is discouraged. Confidential information must be encrypted if copied to or stored on a portable computing device, removable media, or a non-state agency-owned computing device.

The minimum algorithm strength for protecting confidential information is a 128-bit encryption algorithm, subject to state agency risk management decisions justified and documented in accordance with 1 Texas Administrative Code §§ 202.21,202.71(c), 202.25, 202.75.

A state organization may also choose to implement additional protections, which may include encryption, for other data classifications.

SC-15 | COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and

b. Provide an explicit indication of use to users physically present at the devices.

STATE IMPLEMENTATION DETAILS

N/A

SC-20 | SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

STATE IMPLEMENTATION DETAILS

N/A

SC-21 | SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

STATE IMPLEMENTATION DETAILS

N/A

SC-22 | ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

STATE IMPLEMENTATION DETAILS

N/A

SC-39 | PROCESS ISOLATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

Maintain a separate execution domain for each executing system process.

STATE IMPLEMENTATION DETAILS

N/A

SI – SYSTEM AND INFORMATION INTEGRITY

SI-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

SI-2 | FLAW REMEDIATION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [Assignment: organization-defined time-period] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

STATE IMPLEMENTATION DETAILS

The state agency identifies, reports, and corrects information system flaws.

SI-3 | MALICIOUS CODE PROTECTION

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection.

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

STATE IMPLEMENTATION DETAILS

N/A

SI-4 | SYSTEM MONITORING

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and
2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

STATE IMPLEMENTATION DETAILS

Each state agency head or their designated representative and information security officer shall establish a security strategy that includes perimeter protection.

The department will provide security information management services to include external network monitoring, scanning, and alerting for state agencies that utilize State information resources as specified in Texas Government Code Chapters 2054 and 2059. Perimeter security controls may include some or all of the following components: Demilitarized Zone (DMZ), firewall, intrusion detection or prevention system, or router.

SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: No

REQUIRED BY: 01/20/2023

CONTROL DESCRIPTION

a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [Selection (one or more)]: [Assignment: organization-defined personnel or roles] ; [Assignment: organization-defined elements within the organization] ; [Assignment: organization-defined external organizations]; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

STATE IMPLEMENTATION DETAILS

N/A

SI-10 | INFORMATION INPUT VALIDATION

NIST BASELINE: Moderate

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

STATE IMPLEMENTATION DETAILS

N/A

SI-12 | INFORMATION MANAGEMENT AND RETENTION

NIST BASELINE: Low

PRIVACY BASELINE: Yes

NEW REQUIREMENT: No

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

STATE IMPLEMENTATION DETAILS

N/A

SR – SUPPLY CHAIN RISK MANAGEMENT

SR-1 | POLICY AND PROCEDURES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (one or more): organization-level; mission/business process-level; system-level] supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy [Assignment: organization-defined frequency]; and

2. Procedures [Assignment: organization-defined frequency].

STATE IMPLEMENTATION DETAILS

N/A

SR-2 | SUPPLY CHAIN RISK MANAGEMENT PLAN

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];

b. Implement the supply chain risk management plan consistently across the organization; and

c. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes.

STATE IMPLEMENTATION DETAILS

N/A

SR-3 | SUPPLY CHAIN CONTROLS AND PROCESSES

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];

b. Employ the following supply chain controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and

c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].

STATE IMPLEMENTATION DETAILS

N/A

SR-5 | ACQUISITION STRATEGIES, TOOLS, AND METHODS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

STATE IMPLEMENTATION DETAILS

N/A

SR-8 | NOTIFICATION AGREEMENTS

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more)]: notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information].

STATE IMPLEMENTATION DETAILS

N/A

SR-12 | COMPONENT DISPOSAL

NIST BASELINE: Low

PRIVACY BASELINE: No

NEW REQUIREMENT: Yes

REQUIRED BY: 07/20/2023

CONTROL DESCRIPTION

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time-period]; and

b. Automatically [Selection (one or more)]: lock the account or node for an [Assignment: organization-defined time-period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action] when the maximum number of unsuccessful attempts is exceeded.

STATE IMPLEMENTATION DETAILS

N/A