Security Control Standards Catalog

Texas Department of Information Resources

Version 2.1

Effective Date: May 18, 2023

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 may 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. Note, the NIST baseline designation is informational only. All controls contained within this catalog are required for agency systems, regardless of the associated NIST baseline.

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 Texas Administrative Code 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 1 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.
2.1	5/18/2023	DIR Board approval of Version 2.1. Added references, added controls, modified implementation language.

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. Each agency should consider their privacy-related requirements and determine the applicability of the non-mandatory security and privacy controls for agency systems. 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 the **NIST RISK Management Framework**.

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.

Previous Versions of the DIR Control Standards Catalog

Each security control required by previous versions of the DIR Security Control Standards Catalog continues to be required by each state agency until:

(1) the agency has implemented the most recent version of updated control(s) found in this version of the catalog;

(2) the implementation date for each updated control found in this version of the catalog has passed; and/or

(3) the agency can defensibly justify that a previous version of a control is no longer required because it has been effectively superseded or absorbed by a new or additional control in the most recent version of the catalog.

Texas Cybersecurity Framework

DIR developed the Texas Cybersecurity Framework (TCF) in collaboration with other government entities and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies.

The framework is divided into five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. Each functional area contains specific security control objectives to help organizations identify, assess, and manage cybersecurity risks in their environment. The TCF currently consists of 42 total security control objectives.

The TCF is intended to help an organization better understand, manage, and reduce its cybersecurity risks. Part of the TCF structure is determining the maturity of each security control objective. The term "maturity" relates to the degree of implementation and optimization of processes, from nonexistent practices to active optimization of processes.

The TCF is related to the DIR Security Control Standards Catalog but focuses primarily on maturity rather than compliance. Therefore, the assessment of agency maturity against the TCF may require assessing controls beyond the scope of the minimum control standards outlined in this document.

Number of Controls by Family

ID	Control Family	Number of Controls/ Enhancements	Number of Controls/ Enhancements
		Version 2.0	**Version 2.1**
AC	Access Control	13	14
AT	Awareness and Training	4	5
AU	Accountability, Audit, and Risk Management	10	10
CA	Security Assessment and Authorization	9	9
CM	Configuration Management	9	10
CP	Contingency Planning	8	9
IA	Identification and Authentication	10	11
IR	Incident Response	9	9
MA	Maintenance	4	4
MP	Media Protection	4	5
PE	Physical and Environmental Protection	11	11
PL	Planning	3	6
PM	Program Management	12	12
PS	Personnel Security	8	9
RA	Risk Assessment	6	8
SA	System and Service Acquisition	10	10
SC	System and Communication Protection	11	11
SI	System and Information Integrity	7	7
SR	Supply Chain Risk Management	6	6
	Total	**154**	**166**

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.

References: This field provides Texas code and statutory references related to the control. This is an informational field only and is not intended to be an all-inclusive list of references related to the corresponding control.

AC – Access Control

AC-1 | Access Control | Policy and Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC §202.24 (a)(2)

1 TAC §202.74 (a)(2)

AC-2 | Account Management

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

b. Assign account managers;

c. Require [Assignment: organization-defined prerequisites and criteria] 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, prerequisites, and criteria];

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;

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 authenticators (if deployed) when individuals are removed from the group; and

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

State Implementation Details

N/A

References:

None

AC-2(3) | Access Control | Disable Accounts

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Disable accounts within [Assignment: organization-defined time period] when the accounts:

a. Have expired;

b. Are no longer associated with a user or individual;

c. Are in violation of organizational policy; or

d. Have been inactive for [Assignment: organization-defined time period].

State Implementation Details

N/A

References:

None

AC-3 | Access Enforcement

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

AC-5 | Separation Of Duties

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

AC-6 | Least Privilege

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

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 one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.

References:

None

AC-7 | Unsuccessful Logon Attempts

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 must designate at least one threshold activated by invalid logon attempts (i.e., item a from the control description, an agency-defined number of invalid logon attempts by a user account within an agency-defined time-period).
2) As technology permits, state agencies must define, implement, and enforce at least one automatic action that occurs when an agency-defined threshold for invalid logon attempts has been reached (i.e., item b from the control description).
3) In designing and implementing access controls for information systems, state agencies should apply a risk-based approach that considers some or all of the following criteria:
    a. Capabilities and features of the system;
    b. The level of risk presented by the system;
    c. Successful application and enforcement of other security controls, such as multifactor authentication, password entropy, and maturity of other authenticator management practices relevant to the information system;
    d. The ability to detect and mitigate the risk of other types of attacks focused on authentication (e.g., "account spraying" attacks in which threat actors attempt to access multiple accounts from the same IP address or set of IP addresses without causing many failed logon attempts against each individual account targeted by the threat actors);
    e. Whether the system is accessible from the Internet or other public or broadly accessible network(s);
    f. Impacts to the agency's users, operations, and support resources if automatic account lockout controls are abused by threat actors to the determent of account or system availability; and
    g. The application of more rigorous controls commensurate to the value and potential for abuse of a type of account (e.g., applying additional controls, enhancements, or overlays to privileged accounts).

References:

None

AC-8 | System Use Notification

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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 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

N/A

References:

None

AC-14 | Permitted Actions Without Identification Or Authentication

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

Control Description

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

References:

None

AC-17 | Remote Access

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

AC-18 | Wireless Access

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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.

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 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.

References:

None

AC-19 | Access Control For Mobile Devices

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

State organizations shall establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by the state organization or the employee.

References:

Model Security Plan for Prohibited Technologies

AC-20 | Use Of External Systems

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

a. [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [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:

1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [Assignment: organizationally-defined types of external systems].

State Implementation Details

Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. A state agency must require the vendor to periodically provide evidence to the agency that the vendor meets the security controls required under the contract.

References:

Section 2054.138, Government Code

AC-22 | Publicly Accessible Content

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

AT – Awareness and Training

AT-1 | Awareness And Training | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

Section 2054.519, Government Code

1 TAC § 202.24

1 TAC § 202.74

AT-2 | Literacy Training And Awareness

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

a. Provide security and privacy literacy 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 or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];

c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

State Implementation Details

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

References:

Section 2054.519, Government Code

Section 2054.5191, Government Code

Section 2054.5192, Government Code

AT-2(2) | Literacy Training And Awareness | Insider Threat

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Provide literacy training on recognizing and reporting potential indicators of insider threat.

State Implementation Details

N/A

References:

None

AT-3 | Role-Based Training

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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;

b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

State Implementation Details

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

References:

Section 2054.519, Government Code

Section 2054.5191, Government Code

Section 2054.5192, Government Code

AT-4 | Training Records

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

N/A

References:

Section 2054.519, Government Code

Section 2054.5191, Government Code

Section 2054.5192, Government Code

AU – Accountability, Audit, and Risk Management

AU-1 | Audit And Accountability | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

AU-2 | Event Logging

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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-2a.) 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 of, 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 on the risk assessment, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.

References:

1 TAC § 202.25

1 TAC § 202.75

AU-3 | Content Of Audit Records

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

AU-4 | Audit Log Storage Capacity

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

AU-5 | Response To Audit Logging Process Failures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

AU-6 | Audit Record Review, Analysis, And Reporting

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

References:

None

AU-8 | Time Stamps

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

AU-9 | Protection Of Audit Information

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.

State Implementation Details

N/A

References:

None

AU-11 | Audit Record Retention

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

Section 441.185, Government Code

AU-12 | Audit Record Generation

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

CA – Assessment, Authorization, and Monitoring

CA-1 | Assessment, Authorization, And Monitoring | Policies And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

CA-2 | Control Assessments

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. 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;

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

d. 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;

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

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

State Implementation Details

Control assessments shall be conducted at least biennially.

References:

1 TAC §202.26(c)

1 TAC §202.76(c)

CA-3 | Information Exchange

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

Information resources assigned from or shared between one state agency to another or from or between a state agency to a third-party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum.

References:

None

CA-5 | Plan Of Action And Milestones

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 1/20/2023

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, independent audits or reviews, and continuous monitoring activities.

State Implementation Details

N/A

References:

None

CA-6 | Authorization

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

The state organization authorizes the information system for processing before operations or when there is a significant change to the system. A senior organizational official, or their delegate, approves the authorization.

References:

None

CA-7 | Continuous Monitoring

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

1 TAC § 202.27 (c)(1)(B)

1 TAC § 202.77 (c)(1)(B)

CA-7(4) | Continuous Monitoring | Risk Monitoring

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

None

CA-8 | Penetration Testing

NIST Baseline: High

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

Section 2054.516(a)(2), Government Code, 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.

Agencies shall perform, or have performed, an external network penetration test every two years at minimum.

References:

Section 2054.516(a)(2), Government Code

CA-9 | Internal System Connections

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

CM – Configuration Management

CM-1 | Configuration Management | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

CM-2 | Baseline Configuration

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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: organization-defined circumstances]; and
3. When system components are installed or upgraded.

State Implementation Details

N/A

References:

None

CM-3 | Configuration Change Control

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].

State Implementation Details

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

References:

None

CM-4 | Impact Analyses

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

1 TAC § 202.22

1 TAC § 202.72

CM-5 | Access Restrictions For Change

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

CM-6 | Configuration Settings

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

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

References:

None

CM-7 | Least Functionality

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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, system ports, protocols, software, and/or services].

State Implementation Details

N/A

References:

None

CM-8 | System Component Inventory

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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. Does not include duplicate accounting of components or components assigned to any other system;

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

5. 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

References:

Section 2054.068, Government Code

CM-10 | Software Usage Restrictions

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

Model Security Plan for Prohibited Technologies

CM-11 | User-Installed Software

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

1 TAC § 202.22(a)(3)

1 TAC § 202.72(a)(3)

Model Security Plan for Prohibited Technologies

CP – Contingency Planning

CP-1 | Contingency Planning | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

Section 412.054, Labor Code

CP-2 | Contingency Plan

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

a. Develop a contingency plan for the system that:

1. Identifies essential mission 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 mission 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;
6. Addresses the sharing of contingency information; and
7. 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];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

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

State Implementation Details

State agencies shall maintain written Continuity of Operations Plans in compliance with Section 412.054, Labor Code 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.

References:

Section 412.054, Labor Code

CP-3 | Contingency Training

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

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

2. When required by system changes; and

3. [Assignment: organization-defined frequency] thereafter; and

b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

None

CP-4 | Contingency Plan Testing

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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 organization's written disaster recovery plan will include provisions for annual testing.

References:

None

CP-6 | Alternate Storage Site

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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 consistent with agency recovery point objectives and stored in a manner logically and physically segmented from the production environment accessible only to authorized individuals.

References:

None

CP-8 | Telecommunications Services

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

State Implementation Details

N/A

References:

None

CP-9 | System Backup

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

CP-10 | System Recovery And Reconstitution

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

CP-11 | Alternate Communications Protocols

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

IA – Identification and Authentication

IA-1 | Identification And Authentication | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

IA-2 | Identification And Authentication (Organizational Users)

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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.

References:

None

IA-2(1) | Identification And Authentication (Organizational Users) | Multifactor Authentication To Privileged Accounts

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: November 18, 2024

Control Description

Implement multi-factor authentication for access to privileged accounts.

State Implementation Details

N/A

References:

None

IA-2(2) | Identification And Authentication (Organizational Users) | Multifactor Authentication To Non-Privileged Accounts

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

IA-4 | Identifier Management

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

N/A

References:

None

IA-5 | Authenticator Management

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

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

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

State Implementation Details

N/A

References:

None

IA-5(1) | Authenticator Management | Password Based Authentication

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

For password-based authentication:

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

State Implementation Details

N/A

References:

None

IA-6 | Authenticator Feedback

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

IA-7 | Cryptographic Module Authentication

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

IA-8 | Identification And Authentication (Non-Organizational Users)

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

Control Description

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

References:

None

IA-11 | Re-Authentication

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

IR – Incident Response

IR-1 | Incident Response | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

Incident response policies and procedures shall be reviewed and updated at least every two years.

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

IR-2 | Incident Response Training

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

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

2. When required by system changes; and

3. [Assignment: organization-defined frequency] thereafter; and

b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

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

References:

None

IR-3 | Incident Response Testing

NIST Baseline: Moderate

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

Testing includes, but is not limited to the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response and the use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Incident response plans shall be exercised or tested at least annually.

References:

None

IR-4 | Incident Handling

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

1 TAC § 202.23(b)

1 TAC § 202.73(b)

Section 512.053, Business and Commerce Code

IR-5 | Incident Monitoring

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

Track and document incidents.

State Implementation Details

N/A

References:

1 TAC § 202.23(b)

1 TAC § 202.73(b)

Section 512.053, Business and Commerce Code

IR-6 | Incident Reporting

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

b. Report 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) and 1 Texas Administrative Code § 202.73(b).

References:

1 TAC § 202.23(b)

1 TAC § 202.73(b)

Section 512.053, Business and Commerce Code

Section 2054.1125, Government Code

IR-7 | Incident Response Assistance

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 incidents.

State Implementation Details

N/A

References:

None

IR-8 | Incident Response Plan

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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. Addresses the sharing of incident information;
9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and
10. 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

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. Incident response plans shall be reviewed every two years at a minimum.

References:

Section 2054.518, Government Code

IR-9 | Information Spillage Response

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

MA - Maintenance

MA-1 | Maintenance | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

MA-2 | Controlled Maintenance

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

a. Schedule, document, and review records of maintenance, repair, and 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

References:

None

MA-4 | Nonlocal Maintenance

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 authentication 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

References:

None

MA-5 | Maintenance Personnel

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

MP – Media Protection

MP-1 | Media Protection | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

MP-2 | Media Access

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

MP-6 | Media Sanitization

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

N/A

References:

None

MP-6(1) | Media Sanitization | Review, Approve, Track, Document, And Verify

NIST Baseline: High

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Review, approve, track, document, and verify media sanitization and disposal actions.

State Implementation Details

State agencies shall keep a record documenting the removal and completion of sanitization of media that stored confidential information 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.

References:

None

MP-7 | Media Use

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PE – Physical and Environmental Protection

PE-1 | Physical And Environmental Protection | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

The agency shall train designated employees on environmental control procedures, monitoring, and equipment in case of emergencies or equipment problems.

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

PE-2 | Physical Access Authorizations

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PE-3 | Physical Access Control

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 devices]; 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 physical access controls];

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

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

References:

None

PE-6 | Monitoring Physical Access

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PE-8 | Visitor Access Records

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PE-12 | Emergency Lighting

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PE-13 | Fire Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

PE-14 | Environmental Controls

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PE-15 | Water Damage Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PE-16 | Delivery And Removal

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PE-17 | Alternate Work Site

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PL - Planning

PL-1 | Planning | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

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) and § 202.73(a).

References:

1 TAC § 202.23(a)

1 TAC § 202.73(a)

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

PL-2 | System Security And Privacy Plans

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and
15. 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

References:

1 TAC § 202.21(b)(1)

1 TAC § 202.71(b)(1)

Section 2054.133, Government Code

PL-4 | Rules Of Behavior

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

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.

References:

1 TAC § 202.22(a)(3)

1 TAC § 202.72(a)(3)

Section 2054.5191, Government Code

PL-4(1) | Rules Of Behavior | Social Media And External Site/Application Usage Restrictions

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: Yes

Required by: November 18, 2024

Control Description

Include in the rules of behavior, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;
b. Posting organizational information on public websites; and
c. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

State Implementation Details

N/A

References:

Model Security Plan for Prohibited Technologies

PL-10 | Baseline Selection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Select a control baseline for the system.

State Implementation Details

The default baseline for an information system shall be the controls contained in the Security Controls Catalog.

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

(1) contain at least the applicable standards issued by the department; and/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 state agency.

References:

1 TAC § 202.26

1 TAC § 202.76

PL-11 | Baseline Tailoring

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Tailor the selected control baseline by applying specified tailoring actions.

State Implementation Details

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

(1) contain at least the applicable standards issued by the department; and/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 state agency.

References:

1 TAC § 202.26

1 TAC § 202.76

PM – Program Management

PM-1 | Information Security Program Plan

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and

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

State Implementation Details

N/A

References:

1 TAC § 202.24

1 TAC § 202.74

Section 2054.133, Government Code

PM-2 | Information Security Program Role

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 in Section 2054.136, Government Code and 1 Texas Administrative Code § 202.21 and § 202.71.

References:

1 TAC § 202.21

1 TAC § 202.71

Section 2054.136, Government Code

PM-3 | Information Security And Privacy Resources

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

None

PM-4 | Plan Of Action And Milestones Process

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

1. Are developed and maintained;

2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, 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

References:

None

PM-5 | System Inventory

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

Agencies shall update system inventories at least every two years.

References:

Section 2054.068, Government Code

PM-6 | Measures Of Performance

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

PM-7 | Enterprise Architecture

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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, and the Nation.

State Implementation Details

N/A

References:

None

PM-9 | Risk Management Strategy

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

a. Develops a comprehensive strategy to manage:

1. Security risk to organizational operations and assets, individuals, other organizations, 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

References:

1 TAC § 202.24

1 TAC § 202.25

1 TAC § 202.74

1 TAC § 202.75

PM-10 | Authorization Process

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

None

PM-14 | Testing, Training, And Monitoring

NIST Baseline: No Baseline

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

None

PM-15 | Security And Privacy Groups And Associations

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

PM-16 | Threat Awareness Program

NIST Baseline: No Baseline

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

PS – Personnel Security

PS-1 | Personnel Security | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

PS-2 | Position Risk Designation

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

N/A

References:

1 TAC § 202.25

1 TAC § 202.75

PS-3 | Personnel Screening

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PS-4 | Personnel Termination

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

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

References:

None

PS-5 | Personnel Transfer

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

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

References:

None

PS-6 | Access Agreements

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 1/20/2023

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

References:

None

PS-7 | External Personnel Security

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

PS-8 | Personnel Sanctions

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

1 TAC § 202.22(a)(3)

1 TAC § 202.72(a)(3)

PS-9 | Position Descriptions

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

State Implementation Details

N/A

References:

None

RA – Risk Assessment

RA-1 | Risk Assessment | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

RA-2 | Security Categorization

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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.

References:

1 TAC § 202.24(b)(1)

1 TAC § 202.74(b)(1)

1 TAC 202 SUBCHAPTER A

DIR Data Classification Guide

RA-3 | Risk Assessment

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining 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

3. Determining 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, § 202.75, and § 202.77.

References:

1 TAC § 202.25

1 TAC § 202.27

1 TAC § 202.75

1 TAC § 202.77

RA-3(1) | Risk Assessment | Supply Chain Risk Assessment

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

RA-5 | Vulnerability Monitoring And Scanning

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

Section 2058.077, Government Code

RA-5(2) | Vulnerability Monitoring And Scanning | Update Vulnerabilities To Be Scanned

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

State Implementation Details

N/A

References:

Section 2058.077, Government Code

RA-5(11) | Vulnerability Monitoring And Scanning | Public Disclosure Program

NIST Baseline: Low

Privacy Baseline: No

New Requirement: Yes

Required by: November 18, 2024

Control Description

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

State Implementation Details

N/A

References:

None

RA-7 | Risk Response

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

1 TAC § 202.25(4)

1 TAC § 202.75(4)

SA – System and Services Acquisition

SA-1 | System And Services Acquisition | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

SA-2 | Allocation Of Resources

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

None

SA-3 | System Development Life Cycle

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

N/A

References:

None

SA-4 | Acquisition Process

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data for the agency shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency's risk under the contract based on the sensitivity of the agency's data. The vendor must periodically provide to the agency evidence that the vendor meets the security controls required under the contract.

References:

Section 2054.138, Government Code

1 TAC § 202.27

1 TAC § 202.77

SA-5 | System Documentation

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

a. Obtain or develop 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 or develop 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 take [Assignment: organization-defined actions] in response; and

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

State Implementation Details

N/A

References:

None

SA-8 | Security And Privacy Engineering Principles

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SA-9 | External System Services

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

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.

References:

None

SA-10 | Developer Configuration Management

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

N/A

References:

None

SA-11 | Developer Testing And Evaluation

NIST Baseline: Moderate

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 control 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

References:

None

SA-22 | Unsupported System Components

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SC – System and Communications Protection

SC-1 | System And Communications Protection | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

SC-5 | Denial Of Service Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SC-7 | Boundary Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

References:

None

SC-8 | Transmission Confidentiality And Integrity

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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.

References:

None

SC-12 | Cryptographic Key Establishment And Management

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

SC-13 | Cryptographic Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 organization risk management decisions.

Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted.

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.)

Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device.

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

References:

1 TAC § 202.21(c)

1 TAC § 202.71(c)

1 TAC § 202.25

1 TAC § 202.75

SC-15 | Collaborative Computing Devices And Applications

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SC-20 | Secure Name/Address Resolution Service (Authoritative Source)

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

SC-21 | Secure Name/Address Resolution Service (Recursive Or Caching Resolver)

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

SC-22 | Architecture And Provisioning For Name/Address Resolution Service

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

None

SC-39 | Process Isolation

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

Control Description

Maintain a separate execution domain for each executing system process.

State Implementation Details

N/A

References:

None

SI – System and Information Integrity

SI-1 | System And Information Integrity | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

SI-2 | Flaw Remediation

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

N/A

References:

None

SI-3 | Malicious Code Protection

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 and 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; and

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

References:

None

SI-4 | System Monitoring

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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. Analyze detected events and anomalies;

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

N/A

References:

None

SI-5 | Security Alerts, Advisories, And Directives

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 1/20/2023

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

References:

1 TAC § 202.23(b)

1 TAC § 202.73(b)

Section 512.053, Business and Commerce Code

SI-10 | Information Input Validation

NIST Baseline: Moderate

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

State Implementation Details

N/A

References:

None

SI-12 | Information Management And Retention

NIST Baseline: Low

Privacy Baseline: Yes

New Requirement: No

Required by: 7/20/2023

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

References:

Section 441.185, Government Code

1 TAC Chapter 203

13 TAC Chapter 6

Retention Schedules for Texas State Agencies and Public Universities

SR – Supply Chain Risk Management

SR-1 | Supply Chain Risk Management | Policy And Procedures

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 following [Assignment: organization-defined events]; and

2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

State Implementation Details

N/A

References:

1 TAC § 202.24 (a)(2)

1 TAC § 202.74 (a)(2)

SR-2 | Supply Chain Risk Management Plan

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

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

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

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

State Implementation Details

N/A

References:

None

SR-3 | Supply Chain Controls And Processes

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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 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

References:

None

SR-5 | Acquisition Strategies, Tools, And Methods

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SR-8 | Notification Agreements

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

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

References:

None

SR-12 | Component Disposal

NIST Baseline: Low

Privacy Baseline: No

New Requirement: No

Required by: 7/20/2023

Control Description

Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

State Implementation Details

N/A

References:

None

Appendix

Control/Enhancement Additions

Control ID	Control Name	Action
Version 2.0 – January 20, 2022		
CA-7(4)	Continuous Monitoring | Risk Monitoring	Added to Catalog
IA-2(1)	Identification and Authentication (organizational Users) | Multifactor Authentication to Privileged Accounts	Added to Catalog
IA-2(2)	Identification and Authentication (organizational Users) | Multifactor Authentication to Non-privileged Accounts	Added to Catalog
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	Added to Catalog
SR-1	Policy and Procedures	Added to Catalog
SR-12	Component Disposal	Added to Catalog
SR-2	Supply Chain Risk Management Plan	Added to Catalog
SR-3	Supply Chain Controls and Processes	Added to Catalog
SR-5	Acquisition Strategies, Tools, and Methods	Added to Catalog
SR-8	Notification Agreements	Added to Catalog
Version 2.1 – May 18th, 2023		
AC-2(3)	Disable Accounts	Added to Catalog
AT-2(2)	Insider Threat	Added to Catalog
CM-3	Configuration Change Control	Added to Catalog
CP-8	Telecommunications Services	Added to Catalog
IA-5(1)	Password Based Authentication	Added to Catalog
MP-6(1)	Review, Approve, Track, Document, and Verify	Added to Catalog
PL-4(1)	Social Media and External Site/Application Usage Restrictions	Added to Catalog
PL-10	Baseline Selection	Added to Catalog
PL-11	Baseline Tailoring	Added to Catalog
PS-9	Position Descriptions	Added to Catalog
RA-5(2)	Update Vulnerabilities to be Scanned	Added to Catalog
RA-5(11)	Public Disclosure Program	Added to Catalog

Version 2.0 To 2.1 Control Change Summary

ID	Control Name	Low	Mod	High	Privacy	Required by	Changes for version 2.1
AC-1	(Access Control) Policy and Procedures	x			x	7/20/2023	
AC-2	Account Management	x				7/20/2023	Moved implementation details to AC-6
AC-2(3)	Access Control | Disable Accounts	x	x			11/18/2024	New requirement added
AC-3	Access Enforcement	x				1/20/2023	Removed implementation details
AC-5	Separation of Duties	x	x			7/20/2023	
AC-6	Least Privilege	x	x			7/20/2023	Moved implementation details from AC-2 to AC-6
AC-7	Unsuccessful Logon Attempts	x				7/20/2023	Modified implementation details
AC-8	System Use Notification	x				1/20/2023	Removed implementation details
AC-14	Permitted Actions Without Identification or Authentication	x				1/20/2023	
AC-17	Remote Access	x				7/20/2023	
AC-18	Wireless Access	x				7/20/2023	Modified implementation details
AC-19	Access Control for Mobile Devices	x				7/20/2023	Restored implementation details from catalog version 1.3
AC-20	Use of External Systems	x				7/20/2023	Added implementation details
AC-22	Publicly Accessible Content	x				1/20/2023	
AT-1	(Awareness and Training) Policy and Procedures	x			x	7/20/2023	Removed implementation details
AT-2	Literacy Training and Awareness	x			x	7/20/2023	
AT-2(2)	Literacy Training and Awareness | Insider Threat	x				11/18/2024	New requirement added
AT-3	Role-Based Training	x			x	7/20/2023	
AT-4	Training Records	x			x	7/20/2023	Removed implementation details
AU-1	(Audit and Accountability) Policy and Procedures	x			x	7/20/2023	
AU-2	Event Logging	x			x	7/20/2023	
AU-3	Content of Audit Records	x				1/20/2023	
AU-4	Audit Log Storage Capacity	x				7/20/2023	
AU-5	Response to Audit Logging Process Failures	x				7/20/2023	
AU-6	Audit Record Review, Analysis, and Reporting	x				7/20/2023	
AU-8	Time Stamps	x				7/20/2023	
AU-9	Protection of Audit Information	x				7/20/2023	
AU-11	Audit Record Retention	x			x	7/20/2023	
AU-12	Audit Record Generation	x				7/20/2023	

CA-1	(Assessment, Authorization, and Monitoring) Policies and Procedures	x			x	7/20/2023	
CA-2	Control Assessments	x			x	7/20/2023	Modified implementation details
CA-3	Information Exchange	x				7/20/2023	Added implementation details
CA-5	Plan of Action and Milestones	x			x	1/20/2023	
CA-6	Authorization	x			x	7/20/2023	Added implementation details
CA-7	Continuous Monitoring	x			x	7/20/2023	
CA-7(4)	Continuous Monitoring | Risk Monitoring	x			x	7/20/2023	
CA-8	Penetration Testing	x	x	x		7/20/2023	Modified implementation details
CA-9	Internal System Connections	x				7/20/2023	
CM-1	(Configuration Management) Policy and Procedures	x			x	7/20/2023	
CM-2	Baseline Configuration	x				7/20/2023	
CM-3	Configuration Change Control	x	x			11/18/2024	Restored control from catalog version 1.3
CM-4	Impact Analyses	x			x	7/20/2023	Removed implementation details
CM-5	Access Restrictions for Change	x				7/20/2023	
CM-6	Configuration Settings	x				7/20/2023	
CM-7	Least Functionality	x				7/20/2023	
CM-8	System Component Inventory	x				7/20/2023	
CM-10	Software Usage Restrictions	x				1/20/2023	
CM-11	User-Installed Software	x				1/20/2023	
CP-1	(Contingency Planning) Policy and Procedures	x				7/20/2023	Moved implementation details to CP-2
CP-2	Contingency Plan	x				7/20/2023	Moved implementation details from CP-1 to CP-2
CP-3	Contingency Training	x				7/20/2023	
CP-4	Contingency Plan Testing	x				1/20/2023	Modified implementation details
CP-6	Alternate Storage Site	x	x			1/20/2023	Modified implementation details
CP-8	Telecommunications Services	x	x			11/18/2024	Restored control from catalog version 1.3
CP-9	System Backup	x				7/20/2023	
CP-10	System Recovery and Reconstitution	x				7/20/2023	
CP-11	Alternate Communications Protocols					7/20/2023	
IA-1	(Identification and Authentication) Policy and Procedures	x				7/20/2023	
IA-2	Identification and Authentication (Organizational Users)	x				1/20/2023	
IA-2(1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	x				11/18/2024	Aligned control description with NIST language

IA-2(2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	x				7/20/2023	
IA-4	Identifier Management	x				7/20/2023	Moved implementation details to PS4 and PS-5
IA-5	Authenticator Management	x				7/20/2023	
IA-5(1)	Authenticator Management | Password Based Authentication	x				11/18/2024	New requirement added
IA-6	Authenticator Feedback	x				1/20/2023	
IA-7	Cryptographic Module Authentication	x				1/20/2023	
IA-8	Identification and Authentication (Non-Organizational Users)	x				1/20/2023	Added implementation details
IA-11	Re-Authentication	x				7/20/2023	
IR-1	(Incident Response) Policy and Procedures	x			x	7/20/2023	Modified implementation details
IR-2	Incident Response Training	x			x	7/20/2023	Modified implementation details
IR-3	Incident Response Testing	x	x		x	7/20/2023	Modified implementation details
IR-4	Incident Handling	x			x	7/20/2023	
IR-5	Incident Monitoring	x			x	7/20/2023	Aligned control description with NIST language
IR-6	Incident Reporting	x			x	7/20/2023	Modified implementation details
IR-7	Incident Response Assistance	x			x	7/20/2023	Removed implementation details
IR-8	Incident Response Plan	x			x	7/20/2023	Moved implementation details from IR-1 to IR-8
IR-9	Information Spillage Response					7/20/2023	
MA-1	(Maintenance) Policy and Procedures	x				7/20/2023	
MA-2	Controlled Maintenance	x				7/20/2023	
MA-4	Nonlocal Maintenance	x				7/20/2023	
MA-5	Maintenance Personnel	x				1/20/2023	
MP-1	(Media Protection) Policy and Procedures	x			x	7/20/2023	
MP-2	Media Access	x				1/20/2023	
MP-6	Media Sanitization	x			x	7/20/2023	Removed implementation details
MP-6(1)	Media Sanitization | Review, Approve, Track, Document, and Verify	x	x	x		11/18/2024	New requirement added. Added partial implementation details from MP-6.
MP-7	Media Use	x				7/20/2023	
PE-1	(Physical and Environmental Protection) Policy and Procedures	x				7/20/2023	Added implementation details
PE-2	Physical Access Authorizations	x				1/20/2023	
PE-3	Physical Access Control	x				7/20/2023	
PE-6	Monitoring Physical Access	x				1/20/2023	

PE-8	Visitor Access Records	x				7/20/2023	
PE-12	Emergency Lighting	x				1/20/2023	
PE-13	Fire Protection	x				1/20/2023	Removed implementation details
PE-14	Environmental Controls	x				7/20/2023	
PE-15	Water Damage Protection	x				1/20/2023	
PE-16	Delivery and Removal	x				7/20/2023	
PE-17	Alternate Work Site	x	x			7/20/2023	
PL-1	(Planning) Policy and Procedures	x			x	7/20/2023	
PL-2	System Security and Privacy Plans	x			x	7/20/2023	
PL-4	Rules of Behavior	x			x	7/20/2023	Moved implementation details from PS-2 to PL-4
PL-4(1)	Rules of Behavior | Social Media and External Site/Application Usage Restrictions	x			x	11/18/2024	New requirement added
PL-10	Baseline Selection	x				11/18/2024	New requirement added
PL-11	Baseline Tailoring	x				11/18/2024	New requirement added
PM-1	Information Security Program Plan					7/20/2023	
PM-2	Information Security Program Role					7/20/2023	Modified implementation details
PM-3	Information Security and Privacy Resources				x	7/20/2023	
PM-4	Plan of Action and Milestones Process				x	7/20/2023	
PM-5	System Inventory					7/20/2023	Added implementation details
PM-6	Measures of Performance				x	7/20/2023	
PM-7	Enterprise Architecture				x	7/20/2023	
PM-9	Risk Management Strategy				x	7/20/2023	
PM-10	Authorization Process				x	7/20/2023	
PM-14	Testing, Training, and Monitoring				x	7/20/2023	
PM-15	Security and Privacy Groups and Associations					7/20/2023	
PM-16	Threat Awareness Program					7/20/2023	
PS-1	(Personnel Security) Policy and Procedures	x				7/20/2023	
PS-2	Position Risk Designation	x				1/20/2023	Moved implementation details to PL-4
PS-3	Personnel Screening	x				1/20/2023	
PS-4	Personnel Termination	x				7/20/2023	Moved 1A-4 implementation details to PS-4
PS-5	Personnel Transfer	x				1/20/2023	Moved 1A-4 implementation details to PS-5
PS-6	Access Agreements	x			x	1/20/2023	
PS-7	External Personnel Security	x				1/20/2023	
PS-8	Personnel Sanctions	x				1/20/2023	
PS-9	Position Descriptions	x				11/18/2024	New requirement added
RA-1	(Risk Assessment) Policy and Procedures	x			x	7/20/2023	

RA-2	Security Categorization	x				7/20/2023	
RA-3	Risk Assessment	x			x	7/20/2023	Modified implementation details
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	x				7/20/2023	
RA-5	Vulnerability Monitoring and Scanning	x				7/20/2023	Modified implementation details
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned	x				11/18/2024	New requirement added
RA-5(11)	Vulnerability Monitoring and Scanning | Public Disclosure Program	x				11/18/2024	New requirement added
RA-7	Risk Response	x			x	7/20/2023	
SA-1	(System and Services Acquisition) Policy and Procedures	x			x	7/20/2023	
SA-2	Allocation of Resources	x			x	7/20/2023	
SA-3	System Development Life Cycle	x			x	7/20/2023	Removed implementation details
SA-4	Acquisition Process	x			x	7/20/2023	Added implementation details
SA-5	System Documentation	x				7/20/2023	
SA-8	Security and Privacy Engineering Principles	x				7/20/2023	
SA-9	External System Services	x			x	7/20/2023	Moved implementation details from AC-6 to SA-9
SA-10	Developer Configuration Management	x	x			7/20/2023	Removed implementation details
SA-11	Developer Testing and Evaluation	x	x		x	7/20/2023	
SA-22	Unsupported System Components	x				7/20/2023	
SC-1	(System and Communications Protection) Policy and Procedures	x				7/20/2023	
SC-5	Denial of Service Protection	x				7/20/2023	
SC-7	Boundary Protection	x				7/20/2023	
SC-8	Transmission Confidentiality and Integrity	x	x			1/20/2023	Modified implementation details
SC-12	Cryptographic Key Establishment and Management	x				1/20/2023	
SC-13	Cryptographic Protection	x				7/20/2023	Modified implementation details
SC-15	Collaborative Computing Devices and Applications	x				7/20/2023	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	x				1/20/2023	
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	x				1/20/2023	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	x				1/20/2023	
SC-39	Process Isolation	x				1/20/2023	
SI-1	(System and Information Integrity) Policy and Procedures	x			x	7/20/2023	
SI-2	Flaw Remediation	x				1/20/2023	

SI-3	Malicious Code Protection	x				7/20/2023	
SI-4	System Monitoring	x				7/20/2023	Removed implementation details
SI-5	Security Alerts, Advisories, and Directives	x				1/20/2023	
SI-10	Information Input Validation	x	x			7/20/2023	
SI-12	Information Management and Retention	x			x	7/20/2023	
SR-1	(Supply Chain Risk Management) Policy and Procedures	x				7/20/2023	
SR-2	Supply Chain Risk Management Plan	x				7/20/2023	
SR-3	Supply Chain Controls and Processes	x				7/20/2023	
SR-5	Acquisition Strategies, Tools, and Methods	x				7/20/2023	
SR-8	Notification Agreements	x				7/20/2023	
SR-12	Component Disposal	x				7/20/2023	