ENTERPRISE
information services

# Statewide
# Information Technology (IT) Control Standards

January 2024

[This page intentionally left blank]

## AUTHORITY

Oregon Enterprise Information Services (EIS) has the responsibility for developing and overseeing the implementation of statewide information and cyber security standards, and policies relating to information and cyber security, under the authority of Oregon Revised Statute 276A.300. Cyber Security Services (CSS) operates as part of Enterprise Information Services (EIS) and is responsible for creation and maintenance of the Statewide Information and Cyber Security Program Standards.

## APPROVAL

Ben ________________________________________ 01/29/2024

Ben Gherezgiher Date

State of Oregon Chief Information Security Officer

____________________________________________ 1/31/24

Terrence Woods Date

State of Oregon Chief Information Officer

## ACKNOWLEDGEMENTS

Thank you to all who participated and contributed to the review and revision of the standards. The completion of this undertaking could not have been possible without those individuals. Oregon is fortunate to have engagement from dedicated staff across multiple agency who brought their depth of knowledge, different perspectives, and candidness.

# Table of Contents

[This page intentionally left blank]

## EXECUTIVE SUMMARY

Enterprise Information Services (EIS) has established the following IT Control Standards. These Standards facilitate the development, implementation, and operation of secure information and process control systems by establishing a minimum set of controls for accessing, processing, and storing information at defined information asset classification levels, while describing a consistent, comparable, and repeatable approach for layering in security. The controls specified in this document can be referenced by state and agency policies and procedures instead of redefining the same controls within an individual policy or procedure.

EIS has the responsibility for developing and overseeing the implementation of information security policies and statewide standards under the authority of Oregon Revised Statute 276A.300. These Standards address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines. These Standards apply to systems, policies, and procedures within all Executive Branch agencies. Agencies are responsible for complying with these Standards and ensuring that third parties acting on behalf of agencies have formal agreements that guarantee compliance with these Standards.

These Standards provide a catalog of IT controls for State of Oregon information systems to protect state operations, assets, and individuals from a diverse set of threats including malicious acts, natural disasters, structural failures, information system errors and human errors. These Standards support and align with the published Statewide Information Cyber Security Program Plan and applicable statewide policies, including the moderate control families of the National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST SP 800-53 R5).

Individual controls within these Standards specify techniques associated with protecting and securely providing access to the State's information systems. Agencies may elect to exceed these Standards to achieve their organizational security goals and requirements by applying additional controls. The controls documented in these Standards are interdependent and are intended to be implemented in their entirety.

These Standards have been developed using reference documents from the following resources:

*National Institute of Standards and Technology (NIST)*

*State Risk and Authorization Management Program (StateRAMP) Baselines*

*Federal, State, and Local Statues and Rules*

The NIST Glossary of Key Information Security Terms (https://csrc.nist.gov/glossary) is used as the standard reference for terms utilized throughout this document.

*In circumstances where these Standards cannot be implemented, agencies must document deviations and indicate the compensating controls that have been applied to adequately protect systems or information. A deviation document must be signed by the Agency Head as described in the Oregon Statewide Cyber and Information Security Policy (107-004-052).*

## ABOUT THIS DOCUMENT

This document is one component of the Cyber Security Services Program for the State of Oregon. Components of the security program are detailed in the following documents available through the EIS website:

*Statewide Information and Cyber Security Policy (107-004-052)*

*Statewide Information Security Plan*

*Statewide IT Controls Standards (this document)*

*Statewide Incident Response Policy*

The controls selected for these standards have been chosen to reduce cybersecurity risk and constitute the minimum set of controls necessary to meet the requirements for information systems and organizational operations within the State of Oregon. The Standards provide a set of IT controls that must be implemented. Agencies, Boards, and Commissions may need to implement additional controls to meet their specific regulatory needs.

It should be noted that standards within this document utilize an ordinal list structure (letters, numbers, Roman numerals) not for the purpose of implying a particular hierarchy of control elements, but to enable ease of reference.

# STATEWIDE INFORMATION AND CYBER SECURITY STANDARDS

## ACCESS CONTROL – AC

### AC-1 - Policy and Procedures

Policies and procedures for each control family in this document are referenced in the Statewide Information Security Plan (the "Plan"). Individual policies for each control family may be supplied within the Plan or may be published as separate documents. The individual policies reference the applicable controls that are defined in this document.

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### AC-2 - Account Management

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

b. Assign account managers;

c. Require account manager or designee approval 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 organization-defined attributes (as required) for each account;

e. Require approvals by account manager or designee for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with organization-defined policy, procedures, prerequisites, and criteria;

g. Monitor the use of accounts;

h. Notify account manager or designee within:

   1. Twenty-four (24) hours when accounts are no longer required;
   2. Eight (8) hours when users are terminated or transferred; and
   3. Eight (8) hours 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. Applicable federal and state laws and regulations;

j. Review accounts for compliance with account management requirements at least annually;

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.

#### *AC-2(1) - Account Management | Automated System Account Management*

Support the management of system accounts using automated mechanisms.

#### *AC-2(2) - Account Management | Automated Temporary and Emergency Account Management*

Automatically disable temporary and emergency accounts after no more than thirty (30) days.

#### *AC-2(3) - Account Management | Disable Accounts*

Disable accounts within twenty-four (24) hours 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 ninety (90) days

#### *AC-2(4) - Account Management | Automated Audit Actions*

Automatically audit account creation, modification, enabling, disabling, and removal actions.

#### *AC-2(5) - Account Management | Inactivity Logout*

Require that users log out when leaving their workstation unattended.

#### *AC-2(7) - Account Management | Privileged User Accounts*

a. Establish and administer privileged user accounts in accordance with a role-based access scheme;

b. Monitor privileged role or attribute assignments;

c. Monitor changes to roles or attributes; and

d. Revoke access when privileged role or attribute assignments are no longer appropriate.

#### *AC-2(9) - Account Management | Restrictions on Use of Shared and Group Accounts*

Only permit the use of shared and group accounts that meet organization-defined need with justification statement that explains why such accounts are necessary.

#### *AC-2(12) - Account Management | Account Monitoring for Atypical Usage*

a. Monitor system accounts for organization-defined atypical usage; and

b. Report atypical usage of system accounts in accordance with the organization’s Incident Response Plan.

#### *AC-2(13) - Account Management | Disable Accounts for High-Risk Individuals*

Disable accounts of individuals within one (1) hour of discovery of user posing a significant risk.

### AC-3 - Access Enforcement

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

### AC-4 - Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information control flow policies.

***AC-4(21) - Information Flow Enforcement | Physical or Logical Separation of Information Flows***

Separate information flows logically or physically using organization-defined mechanisms and/or techniques to accomplish required separations by types of information.

## AC-5 - Separation of Duties

a. Identify and document roles and permissions; and

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

## AC-6 - Least Privilege

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

***AC-6(1) - Least Privilege | Authorize Access to Security Functions***

Authorize access for privileged users to:

a. Security functions; and

b. Security-relevant information.

***AC-6(2) - Least Privilege | Non-privileged Access for Non-security Functions***

Require that users of system accounts (or roles) with access to all security functions use non-privileged accounts or roles, when accessing non-security functions.

***AC-6(5) - Least Privilege | Privileged Accounts***

Restrict privileged accounts on the system to authorized individuals with a need for elevated privileges.

***AC-6(7) - Least Privilege | Review of User Privileges***

a. Review the privileges assigned to all users with privileges at least annually to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

***AC-6(9) - Least Privilege | Log Use of Privileged Functions***

Log the execution of privileged functions.

***AC-6(10) - Least Privilege | Prohibit Non-privileged Users From Executing Privileged Functions***

Prevent non-privileged users from executing privileged functions.

## AC-7 - Unsuccessful Logon Attempts

a. Enforce a limit of no more than three (3) consecutive invalid logon attempts by a user during a fifteen (15) minute period;

    1. For mobile devices: not more than ten (10) consecutive invalid attempts; and

b. Automatically lock the account or node for a minimum of thirty (30) minutes or until unlocked by an administrator.

### AC-8 - System Use Notification

Prior to granting access to the system, display to users an approved system use notification that provides privacy and security notices consistent with applicable federal and state laws. Executive Orders, directives, policies, regulations, standards, and guidance.

a. The system use notification message shall, at a minimum, provide the following information:

    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 notification, 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.

### AC-11 - Device Lock

a. Prevent further access to the system by:

    1. Initiating a device lock after fifteen (15) minutes of inactivity

        i) For mobile devices, five (5) minutes; and

    2. Requiring the user to initiate a device lock before leaving the system unattended; and

b. Retain the device lock until the authorized user reestablishes access using identification and authentication procedures.

#### *AC-11(1) - Device Lock | Pattern Hiding Displays*

Conceal, via the device lock, information previously visible on the display, with a publicly viewable image.

### AC-12 - Session Termination

Automatically terminate user sessions after thirty (30) minutes of inactivity, unless otherwise defined in the applicable System Security Plan (SSP).

### AC-14 - Permitted Actions without Identification or Authentication

a. Identify specific user actions that can be performed on the system without identification or authentication consistent with agency missions and business functions; and

b. Document and provide supporting rationale in SSPs for user actions that do not require identification or authorization.

## AC-17 - Remote Access

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.

### *AC-17(1) - Remote Access | Monitoring and Control*

Employ automated mechanisms to monitor and control remote access methods.

### *AC-17(2) - Remote Access | Protection of Confidentiality / Integrity Using Encryption*

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

### *AC-17(3) - Remote Access | Managed Access Control Points*

Route all remote accesses through authorized and managed network access control points.

### *AC-17(4) - Remote Access | Privileged Commands / Access*

a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and when there is a compelling business need; and

b. Document the rationale for such access in the SSP.

## AC-18 - Wireless Access

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.

### *AC-18(1) - Wireless Access | Authentication and Encryption*

Protect wireless access to the system using authentication of both user and devices, and encryption.

### *AC-18(3) - Wireless Access | Disable Wireless Networking*

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

## AC-19 - Access Control for Mobile Devices

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.

### *AC-19(5) - Access Control for Mobile Devices | Full Device / Container-based Encryption*

Employ full-device encryption to protect the confidentiality and integrity of information on all mobile devices.

## AC-20 - Use of External Systems

Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and / or maintaining external systems, allowing authorized individuals to:

a. Access internal information systems or system components from external systems; and

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

### *AC-20(1) - Use of External Systems | Limits on Authorized Use*

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

a. Verification of the implementation of controls on the external system as specified in the Organization's security policies and plans; or

b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

### *AC-20(2) - Use of External Systems | Portable Storage Devices*

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using agency documented and approved restrictions.

## AC-21 - Information Sharing

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances where user discretion is required; and

b. Employ automated mechanisms or manual processes compliant with agency requirements to assist users in making information sharing and collaboration decisions.

## AC-22 - Publicly Accessible Content

a. Designate individuals that are authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain non-public 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 content on the publicly accessible system for non-public information at least quarterly and remove such information, if discovered.

## AWARENESS AND TRAINING – AT

### AT-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### AT-2 - Security Awareness and Training

a. Provide security literacy training to system users (including managers, senior executives, and contractors):
   1. As part of initial training for new users and at least annually thereafter; and
   2. When required by system changes or following significant events;

b. Employ supplement training as necessary to increase the security awareness of system users and to meet regulatory and compliance obligations;

c. Update literacy training and awareness content at least annually and following significant events; and

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

#### *AT-2(2) - Security Awareness and Training | Insider Threat*

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

#### *AT-2(3) - Security Awareness Training | Social Engineering and Data Mining*

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

### AT-3 - Role-Based Training

a. Provide role-based security training to software development personnel; personnel with privileged access; and other personnel as required by applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance:
   1. Before authorizing access to the system, information, or performing assigned duties, and at least annually thereafter; and
   2. When required by system changes;

b. Update role-based training content at least annually and following significant events; and

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

### AT-4 - Security Training Records

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

b. Retain individual training records for at least one (1) year or one (1) year after completion of a specific training program.

## AUDIT AND ACCOUNTABILITY – AU

### AU-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### AU-2 - Events Logging

a. Identify the types of events that systems are capable of logging in support of the audit function that, at a minimum, includes:

   1. For on-premises applications:

      i) successful and unsuccessful account logon events;

      ii) account management events;

      iii) object access;

      iv) policy change;

      v) privilege functions;

      vi) process tracking; and

      vii) system events.

   2. For Web applications:

      i) all administrator activity;

      ii) authentication checks;

      iii) authorization checks;

      iv) data deletions;

      v) data access;

      vi) data changes; and

      vii) permission changes;

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 event types for logging within the system consisting of a subset of the event types defined in AU-2 (a), along with the frequency of (or situation requiring) logging for each identified event type;

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

e. Review and update the event types selected for logging at least annually, or when a major change to the system occurs.

### AU-3 - Content of Audit Records

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.

***AU-3(1) - Content of Audit Records | Additional Audit Information***

Generate audit records containing the information necessary to facilitate the reconstruction of events in the event (or suspected event) of unauthorized activity or malfunction.

## AU-4 - Audit Storage Capacity

Allocate audit log storage capacity to accommodate State of Oregon records retention schedules and any other applicable retention requirements.

## AU-5 - Response to Audit Processing Failures

a. Alert agency designated personnel or roles when the event of an audit logging process failure; and

b. Overwrite oldest record(s).

## AU-6 - Audit Review, Analysis, and Reporting

a. Review and analyze system audit records at least weekly for indications of inappropriate or unusual activity;

b. Report findings to appropriate organization according to agency, State of Oregon, and Federal Incident Response Policy and procedures; 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.

***AU-6(1) - Audit Review, Analysis, and Reporting | Process Integration***

Integrate audit record review, analysis, and reporting processes.

***AU-6(3) - Audit Review, Analysis, and Reporting | Correlate Audit Repositories***

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

## AU-7 - Audit Reduction and Report Generation

Provide and implement an audit reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

***AU-7(1) - Audit Reduction and Report Generation | Automatic Processing***

Provide and implement the capability to process, sort, and search audit records for events of interest based on individual items, or combinations of items contained in the audit records, as defined in AU-3.

## AU-8 - Time Stamps

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

b. Record time stamps for audit records that meet 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.

### AU-9 - Protection of Audit Information

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

b. Alert the Organization assigned personnel upon detection of unauthorized access, modification, or deletion of audit information.

#### *AU-9(4) - Protection of Audit Information | Access by Subset of Privileged Users*

Authorize access to management of audit logging functionality to only personnel that have a need to know and have been expressly authorized for this function.

### AU-11 - Audit Record Retention

Retain audit records for at least ninety (90) days to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

### AU-12 - Audit Record Generation

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all information system and network components where audit capability is deployed/available;

b. Allow agency system owners, agency information owners, or system security administrators 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-2 that include the audit record content defined in AU-3.

## ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

### CA-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### CA-2 - Security Assessments

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 (AO) or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation at least annually, or when there is a significant change to the system, 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 requirements;

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

f. Provide the results of the control assessment to AO and other parties as described in the Oregon Statewide Information Security Plan.

#### *CA-2(1) - Control Assessments | Independent Assessors*

Employ independent assessors or assessment teams to conduct control assessment.

#### *CA-2(3) - Control Assessments | Leveraging Results from External Organizations*

Leverage the results of control assessments performed by external organizations.

### CA-3 - System Interconnections

a. Approve and manage the exchange of information between the system and other systems by means of formal agreements (e.g., interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, or nondisclosure agreements);

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

c. Review and update the agreements annually.

### CA-5 - Plan of Action and Milestones

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 at least monthly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

## CA-6 - Authorization

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

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

c. Ensure that the AO 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; and

e. Update the authorizations at least every three (3) years or when a significant change occurs.

## CA-7 - Continuous Monitoring

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 system-level metrics to be monitored and documented in the applicable SSP;

b. Establishing organization-defined frequencies (no less than annually) for monitoring and organization-defined frequencies (no less than annually) 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 status of the system to the Agency Director, or designee thereof, at least annually.

### *CA-7(1) - Continuous Monitoring | Independent Assessors*

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

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

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.

## CA-8 - Penetration Testing

Conduct penetration testing at least annually.

***CA-8(1) - Penetration Testing | Independent Penetration Testing Agent or Team***

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

***CA-8(2) - Penetration Testing | Red Team Exercises***

Employ red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement.

## CA-9 - Internal System Connections

a. Authorize internal connections of intra-system components to the system;

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

c. Terminate internal system connections according to the session limit standards as specified under AC-12 and SC-10; and

d. Review annually the continued need for each internal connection.

## CONFIGURATION MANAGEMENT (CM)

### CM-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### CM-2 - Baseline Configuration

a. Develop, document, and maintain current baseline configurations;

b. Review and update the baseline configurations:

   1. At least annually or when a significant change occurs;
   2. When required due to compliance requirement or direction from an authoritative body; and
   3. When system components are installed or upgraded.

#### *CM-2(2) - Baseline Configuration | Automation Support for Accuracy and Currency*

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using organization-defined automated mechanisms.

#### *CM-2(3) - Baseline Configuration | Retention of Previous Configurations*

Retain secure images or templates, according to approved configuration standards, for all systems in the enterprise, of previous versions of baseline configurations of the system to support rollback.

#### *CM-2(7) - Baseline Configuration | Configure Systems and Components For High-Risk Areas*

State devices may only be used when traveling for approved state business; State-owned devices are not allowed to travel with an employee on personal travel outside of the country without prior CSS consultation.

a. When travelling internationally to countries sanctioned by the United States Treasury (https://ofac.treasury.gov/sanctions-programs-and-country-information) or United States State Department (https://www.state.gov/economic-sanctions-programs/):

   1. All state business must be performed using a onetime use or burner device:

      i) Onetime use or burner devices will have no access to state networks;

      ii) Passwords for onetime use or burner devices must be different than daily Active Directory (AD) password;

      iii) Username and password for onetime use or burner devices must not match any other account login and be unique; and

      iv) Full disk encryption for onetime use or burner devices (Full disk encryption may be illegal in some countries. Please consult with DOJ before travel begins); and

   2. Access to Enterprise Cloud Platforms is prohibited;

b. When travelling internationally to non-sanctioned countries, devices that contain data classified as level 3 or above may only contain that data which is necessary for the purpose associated with the travel. Any state-issued and -managed device must be hardened according to the Statewide Information Technology Control Standards. Additionally,

2. Full disk encryption must be implemented on laptops and other portable computing devices (Full disk encryption may be illegal in some countries. Please consult with DOJ before travel begins);
3. Personnel must use VPN to access state networks; and
4. State-managed mobile devices (e.g., tablets, cell phones) must be enrolled in mobile device management (MDM);

c. Upon return from travel to a sanctioned country, user passwords must be reset and devices must be returned to organizational information technology support personnel to perform the following actions:

1. Devices must not connect to internal networks;
2. Any data must be copied to external media and scanned for malware before transferring to state network or managed devices;
3. Devices must be re-image before returning to checkout status, if applicable; and

d. Upon return from travel to a non-sanctioned country:

1. Device must be re-imaged before connecting to the state network; and
2. User passwords must be reset before returning to work.

## CM-3 - Configuration Change Control

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

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security 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 systems according to applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance;

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 regular change control meeting that convenes: The frequency of these meetings is dependent upon the needs of the agency and should take into account the typical number and impact of changes.

### *CM-3(2) - Configuration Change Control | Test / Validate / Document Changes*

Test, validate, and document changes to the system before finalizing the implementation of the changes.

### *CM-3(4) - Configuration Change Control | Security Representative*

Require security representation as a part of the change advisory board or process.

## CM-4 - Security Impact Analyses

Analyze changes to systems to determine potential security impacts prior to change implementation.

### *CM-4(2) - Security Impact Analysis | Verification of Security Functions*

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

## CM-5 - Access Restrictions for Change

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

### *CM-5(1) - Access Restrictions for Change | Automated Access Enforcement and Audit Records*

a. Enforce access restrictions using automated mechanisms; and

b. Automatically generate audit records of the enforcement actions.

### *CM-5(5) - Access Restrictions for Change | Privilege Limitation for Production and Operation*

a. Limit privileges to change system components and system-related information within a production or operational environment; and

b. Review and reevaluate privileges at least quarterly.

## CM-6 - Configuration Settings

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using CIS Level 1 Benchmark;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for components within the system based on operational requirements; and

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

### *CM-6(1) - Configuration Settings | Automated Management, Application, and Verification*

Manage, apply, and verify configuration settings using organization-defined automated mechanisms.

## CM-7 - Least Functionality

a. Configure the system to provide only essential capabilities;

b. Disable or remove by default, all network ports, protocols, server roles, software, and services.

### *CM-7(1) - Least Functionality | Periodic Review*

a. Review systems at least annually to identify unnecessary and / or non-secure functions, ports, protocols, software, and services; and

b. Disable or remove by default, all network ports, protocols, server roles, software, and services.

### *CM-7(2) - Least Functionality | Prevent Program Execution*

Prevent program execution in accordance with the Organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

### *CM-7(5) - Least Functionality | Authorized Software – Allow by Exception*

a. Identify and maintain a current inventory of all software assets that are authorized to execute on the system;

b. Employ a deny-all, permit-by-exception methodology to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs at least annually or when there is a change.

## CM-8 - System Component Inventory

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

   1. Accurately reflects the current 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 organization-defined information deemed necessary to achieve effective system component accountability; and

b. Review and update the system component inventory at least monthly.

### *CM-8(1) - System Component Inventory | Updates During Installation / Removals*

Update the inventory of system components as part of component installations, removals, and system updates.

### *CM-8(3) - System Component Inventory | Automated Unauthorized Component Detection*

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms with a maximum five-minute delay in detection; and

b. Remove or quarantine unauthorized components from the network when unauthorized components are detected.

## CM-9 - Configuration Management Plan

Develop, document, and implement a configuration management plan for the systems, that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the System Development Life Cycle (SDLC) and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by the Agency Chief Information Officer (CIO) or equivalent, or designee thereof; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

### CM-10 - Software Usage Restrictions

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 technologies to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

### CM-11 - User-installed Software

a. Establish policies governing the installation of software by users;

b. Enforce software installation policies through procedural and automated methods; and

c. Monitor policy compliance continuously.

### CM-12 - Information Location

a. Identify and document the location of a data inventory, based on the enterprise data governance policy and the specific system components on which the information is processed and stored;

b. Identify and document users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

#### *CM-12(1) - Information Location | Automated Tools to Support Information Location*

Use automated tools to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory to ensure controls are in place to protect organizational information.

## CONTINGENCY PLANNING (CP)

### CP-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### CP-2 - Contingency Plan

a. Develop a contingency plan for the system(s) that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by the Agency Head or equivalent;

b. Distribute copies of the contingency plan to key contingency personnel;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system at least annually;

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 key contingency personnel;

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 modification and disclosure.

#### *CP-2(1) - Contingency Plan | Coordinate with Related Plans*

Coordinate contingency plan development with organizational elements responsible for related plans.

#### *CP-2(3) - Contingency Plan | Resume Essential Missions / Business Functions*

Plan for the resumption of all mission and business functions within time periods documented in the Continuity Plan of contingency plan activation.

#### *CP-2(8) - Contingency Plan | Identify Critical Assets*

Identify and document critical system assets supporting essential mission and business functions.

### CP-3 - Contingency Training

a. Provide contingency training to system users consistent with their assigned contingency roles and responsibilities:
   1. Within ten (10) days of assuming a contingency role or responsibility;
   2. When required by system changes; and

3. At least annually thereafter; and

b. Review and update contingency training content at least annually and following significant events.

### CP-4 - Contingency Plan Testing

a. Perform a functional exercise at least annually to test the contingency plan for the system to determine the effectiveness of the plan and the readiness to execute the plan;

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

#### *CP-4(1) - Contingency Plan Testing | Coordinate With Related Plans*

Coordinate Contingency Plan testing with organizational elements responsible for related plans.

### CP-6 - Alternate Storage Site

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 security controls equivalent to that of the primary site.

#### *CP-6(1) - Alternate Storage Site | Separation from Primary Site*

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

#### *CP-6(3) - Alternate Storage Site | Accessibility*

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

### CP-7 - Alternate Processing Site

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of system operations for essential missions and business functions within time-periods consistent with organization-defined recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the Organization-defined time-period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

#### *CP-7(1) - Alternate Processing Site | Separation from Primary Site*

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

#### *CP-7(2) - Alternate Processing Site | Accessibility*

Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

### *CP-7(3) - Alternate Processing Site | Priority of Service*

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

## CP-8 - Telecommunications Service

Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within agency-defined recovery time and recovery point objectives when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

### *CP-8(1) - Telecommunications Service | Priority of Service Provisions*

a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

### *CP-8(2) - Telecommunications Service | Single Points of Failure*

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

## CP-9 - System Backup

a. Conduct full backups of user-level information contained in the system weekly, with incremental daily;
b. Conduct full backups of system-level information contained in the system weekly, with incremental daily;
c. Conduct full backups of system documentation, including security-related documentation weekly, with incremental daily; and
d. Protect the confidentiality, integrity and availability of backup information.

### *CP-9(1) - System Backup | Testing for Reliability and Integrity*

Test backup information at least annually to verify media reliability and information integrity.

### *CP-9(8) - System Backup | Cryptographic Protection*

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files.

## CP-10 - System Recovery and Reconstruction

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

### *CP-10(2) - System Recovery and Reconstruction | Transaction Recovery*

Implement transaction recovery for systems that are transaction-based.

## IDENTIFICATION AND AUTHENTICATION (IA)

### IA-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### IA-2 - Identification and Authentication (Organizational Users)

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

***IA-2(1) - Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts***

Implement multi-factor authentication for access to privileged accounts.

***IA-2(2) - Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-privileged Accounts***

Implement multi-factor authentication for access to non-privileged accounts.

***IA-2(5) - Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication***

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

***IA-2(6) - Identification and Authentication (organizational Users) | Access to Accounts – Separate Device***

Implement multi-factor authentication for local, network, or remote access to privileged and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and
b. The device meets organization-defined strength of mechanism requirements.

***IA-2(8) - Identification and Authentication (Organizational users) | Access to Accounts – Replay Resistant***

Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts.

***IA-2(12) - Identification and Authentication (Organizational users) | Acceptance of PIV Credentials***

Accept and electronically verify Personal Identity Verification (PIV)-compliant credentials for applicable Federal Systems.

### IA-3 - Device-Level Identification and Authentication

Uniquely identify and authenticate end user-operated devices, including devices that are not owned by the Organization, before accessing agency information assets.

### IA-4 - Identifier Management

Manage system identifiers by:

a. Receiving authorization from the documented agency designated approving authority to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group role, or device; and
d. Preventing reuse of identifiers for at least two (2) years.

***IA-4(4) - Identifier Management | Identify User Status***

Manage individual identifiers by uniquely identifying each individual status including contractors, foreign nationals, and non-organizational users.

## IA-5 - Authenticator Management

Manage system authenticators as follows:

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 at least every ninety (90) days or when authenticators are shared, reported lost, stolen, or compromised;
g. Protecting authenticator content from unauthorized disclosure and modification;
h. Requiring individuals to take, and have devices implement, specific controls to protect authenticators; and
i. Changing authenticators for group or role accounts when membership to those accounts changes.

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

For password-based authentication:

a. Maintain a list of commonly used, expected, or compromised passwords and update the list at least every three (3) years 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;
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;

h. Enforce the following composition and complexity rules:
   1. Enforce minimum password length of fifteen (15) characters;
   2. Enforce minimum password complexity to contain at least:
      i) One (1) numeric (e.g., zero – 9);
      ii) One (1) non-alphanumeric character (e.g., @, #, $, %, ^, &, etc.);
      iii) One (1) English uppercase letter (e.g., A – Z); and
      iv) One (1) English lowercase letter (e.g., a – z);
   3. No dictionary words or common names;
   4. No portions of the associated account name / identifier (e.g., User I.D., login name); and
   5. Enforce at least one (1) character change when new passwords are selected for use;

i. Store and transmit only cryptographically protected passwords;

j. Enforce password lifetime restrictions:
   1. One (1) day minimum and sixty (60) days maximum; and
   2. Service accounts passwords shall expire within three hundred sixty-six 366 days (inclusive);

k. Password History/Reuse:
   1. For all systems: twenty-four (24) generations; and
   2. For systems unable to implement history/reuse restriction by generations but are able to restrict history/reuse for a specified time period, passwords shall not be reusable for a period of six (6) months;

l. Allow the use of a temporary password for system logons with an immediate change to a permanent password;

m. Map the authenticated identity to the account of the individual or group; and

n. Implement a local cache of revocation data to support path discovery and validation.

***IA-5(2) - Authenticator Management | PKI Based Authentication***

a. For public key-based authentication:
   1. Enforce authorized access to the corresponding private key; and
   2. Map the authenticated identity to the account of the individual or group; and.

b. When Public Key Infrastructure (PKI) is used:
   1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
   2. Implement a local cache of revocation data to support path discovery and validation.

***IA-5(6) - Authenticator Management | Protection of Authenticators***

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

***IA-5(7) - Authenticator Management | No Embedded Unencrypted Static Authenticators***

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

## IA-6 - Authenticator Feedback

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

## IA-7 - Cryptographic Module Authentication

Implement mechanisms for authentication to a cryptographic module that will meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

## IA-8 - Identification and Authentication (Non-Organizational Users)

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

***IA-8(1) - Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from other agencies***

Accept and electronically verify PIV-compliant credentials from other federal agencies for applicable federal systems.

***IA-8(2) - Identification and Authentication (Non-Organizational Users) | Acceptance of External Authentication***

**For applicable federal systems:**

a. Accept only external authenticators that are NIST-compliant; and

b. Document and maintain a list of accepted external authenticators.

***IA-8(4) - Identification and Authentication (Non-Organizational Users) | Use of FICAM- Issued Profiles***

Conform to organization-defined identity management profiles.

## IA-11 - Identification and Authentication | Re-Authentication

Require users to re-authenticate:

a. When roles, authenticators or credentials change;

b. When execution of privileged functions occurs; or

c. Within 7 days of previous authentication; and

d. Within twenty-four (24) hours of previous authentication.

## IA-12 - Identity Proofing

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

***IA-12(2) - Identity Proofing | Identity Evidence***

Require evidence of individual identification.

***IA-12(3) - Identity Proofing | Identity Evidence Validation and Verification***

Require that the presented identity evidence be validated and verified through organizational defined methods of validation and verification.

***IA-12(5) - Identity Proofing | Address Confirmation***

Require that a notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

## INCIDENT RESPONSE – IR

### IR-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### IR-2 - Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
    1. Within ten (10) days of assuming an incident response role or responsibility or acquiring system access;
    2. When required by system changes; and
    3. At least annually thereafter; and

b. Review and update incident response training content at least annually and following significant events.

### IR-3 - Incident Response Testing

Perform functional testing of the effectiveness of the incident response capability for the system at least annually.

***IR-3(2) - Incident Response Testing | Coordination With Related Plans***

Coordinate incident response testing with organizational elements responsible for related plans.

### IR-4 - Incident Handling

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, 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.

***IR-4(1) - Incident Handling | Automated Incident Handling Processes***

Support the incident handling process using automated mechanisms to support the incident handling processes.

### IR-5 - Incident Monitoring

Track and document incidents.

### IR-6 - Incident Reporting

a. Require personnel to report suspected incidents to the organizational incident response capability as soon as possible, but in no case later than one (1) hour following discovery; and

b. Report incident information to internal agency incident response resources.

### *IR-6(1) - Incident Reporting | Automated Reporting*

Report incidents using organization-defined process.

### *IR-6(3) - Supply Chain Coordination*

Provide security incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

## IR-7 - Incident Response Assistance

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.

### *IR-7(1) - Incident Response Assistance | Automation Support for Availability of Information and Support*

Increase the availability of incident response information and support using automated mechanisms to support the incident handling processes.

## IR-8 - Incident Response Plan

a. Develop an Incident Response Plan that:
   1. Provides agencies with a roadmap for implementing an 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 agency senior leadership, and applicable Incident Response Team (IRT) leaders and personnel annually; and
   10. Explicitly designates responsibility for incident response to agency senior leadership, and applicable IRT leaders and personnel.

b. Distribute copies of the incident response plan to agency senior leadership, and applicable IRT leaders and personnel;

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 agency senior leadership, and applicable IRT leaders and personnel; and

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

## IR-9 - Information Spillage Response

Respond to information spills by:

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

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

c. Alerting 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. Reporting incident information in accordance with the Incident Response Plan.

### *IR-9(2) - Information Spillage Response | Training*

Provide information spillage response training at least annually.

### *IR-9(3) - Information Spillage Response | Post-spill Operations*

Implement procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

### *IR-9(4) - Information Spillage Response | Exposure to Unauthorized Personnel*

Employ controls for personnel exposed to information not within assigned access authorizations.

## MAINTENANCE (MA)

### MA-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### MA-2 - Controlled Maintenance

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 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 organization-defined information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;

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

f. Include organization-defined information in maintenance records.

### MA-3 - Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools at least annually.

#### *MA-3(1) - Maintenance Tools | Inspect Tools*

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

#### *MA-3(2) - Maintenance Tools | Inspect Media*

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

#### *MA-3(3) - Maintenance Tools | Prevent Unauthorized Removal*

Prevent the removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment;

b. Sanitizing or destroying the equipment;

c. Retaining the equipment within the facility; or

d. Obtaining an exemption from the information owner explicitly authorizing removal of the equipment from the facility.

### MA-4 - Non-local Maintenance

a. Approve and monitor all non-local maintenance and diagnostic activities performed on agency systems;

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

c. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

d. Maintain records of non-local maintenance and diagnostic activities; and

e. Terminate all sessions and network connections when non-local maintenance is completed.

### MA-5 - Maintenance Personnel

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.

#### *MA-5(1) - Maintenance Personnel | Individuals Without Appropriate Access*

The organization:

a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

### MA-6 - Timely Maintenance

Obtain maintenance support and/or spare parts in sufficient time to meet recovery time objectives of failure.

## MEDIA PROTECTION (MP)

### MP-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### MP-2 - Media Access

Restrict access to all digital and non-digital media to authorized personnel only.

### MP-3 - Media Marking

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempt no removeable media from marking (even if the media remain within organization-defined controlled areas).

### MP-4 - Media Storage

a. Physically control and securely store all types of digital and/or non-digital media with sensitive information within organization-defined controlled areas using defined security measures; and
b. Protect system media types defined above until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

### MP-5 - Media Transport

a. Protect and control all media with sensitive information during transport outside of controlled areas using organization-defined security measures;
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

### MP-6 - Media Sanitization

a. Sanitize all system media (both digital and non-digital) prior to disposal, release out of organizational control, or release for reuse using State approved equipment, techniques, and procedures; and
b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

### MP-7 - Media Use

a. Prohibit the use of any non-approved media on state systems using organization-defined controls; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

## PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

### PE-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### PE-2 - Physical Access Authorizations

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 at least annually; and

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

### PE-3 - Physical Access Control

a. Enforce physical access authorizations for all physical access points (including designated entry and exit points) to areas where systems reside by:

   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress and egress to the facility using organization-defined physical access control systems/devices;

b. Maintain physical access audit logs for organization-defined entry and exit points;

c. Control access to areas within the facility designated as publicly accessible by implementing organization-defined physical access controls;

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

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

f. Inventory physical access devices at least annually; and

g. Change combinations and keys at least annually and/or when keys are lost, combinations are compromised, or when individuals processing the keys or combinations are transferred or terminated.

### PE-4 - Access Control for Transmission

Control physical access to system distribution and transmission lines within organizational facilities using protective measures to control physical access to information system distribution and transmission lines, such as:

a. Locked wiring closets;

b. Disconnected or locked spare jacks; and

c. Protection of cabling by conduit or cable trays.

### PE-5 - Access Control for Output Devices

Control physical access to output from organization-defined output devices to prevent unauthorized individuals from obtaining the output.

### PE-6 - Monitoring Physical Access

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

b. Review physical access logs at least monthly and upon indications of inappropriate or unusual activity; and

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

#### *PE-6(1) - Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment*

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

### PE-8 - Visitor Access Records

a. Maintain visitor access records for the facility where the system resides for a minimum of one (1) year;

b. Review visitor access records at least monthly; and

c. Report anomalies in visitor access records to organization-defined personnel.

### PE-9 - Power Equipment and Cabling

Protect power equipment and power cabling for the system from damage and destruction.

### PE-10 - Emergency Shutoff

a. Provide the capability of shutting off power to the system or individual system components in emergency situations;

b. Place emergency shutoff switches or devices in locations as defined by applicable standards, to facilitate safe and easy access for personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

### PE-11 - Emergency Power

Provide an uninterruptible power supply to facilitate an orderly shutdown of the system or transition of the system to long-term alternate power in the event of a primary power source loss.

### PE-12 - Emergency Lighting

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.

### PE-13 - Fire Protection

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

#### *PE-13(1) - Fire Protection | Detection Systems – Automatic Activation and Notification*

Employ fire detection systems that activate automatically and notify organization-defined personnel or roles and emergency responders in the event of a fire.

### *PE-13(2) - Fire Protection | Suppression Systems — Automatic Activation and Notification*

a. a. Employ fire suppression systems that activate automatically and notify organization-defined personnel or roles (including emergency responders); and

b. b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

## PE-14 - Environmental Controls

a. Maintain the temperature and humidity levels within the facility where the system resides within limits as documented by the equipment manufacturer; and

b. Monitor environmental control levels continuously.

## PE-15 - Water Damage Protection

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.

## PE-16 - Delivery and Removal

a. Authorize and control all system components entering and exiting the facility; and

b. Maintain records of the system components.

## PE-17 - Alternate Work Site

a. Determine and document the alternate worksites allowed for use by employees;

b. Employ statewide and agency security controls at alternate work sites;

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

d. Provide a means to communicate with information security personnel in case of incidents.

## PLANNING (PL)

### PL-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### PL-2 - Security Plans

a. Develop security 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. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
    9. Provide an overview of the security requirements for the system;
    10. Identify any relevant control baselines or overlays, if applicable;
    11. Describe the controls in place or planned for meeting the security requirements, including a rationale for any tailoring decisions;
    12. Include risk determinations for security architecture and design decisions;
    13. Include security-related activities affecting the system that require planning and coordination with authorized agency personnel, including individuals or groups as identified in organization plans (including SSPs), contingency plans, and incident response plans); and
    14. Are reviewed and approved by the AO or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to designated personnel;

c. Review the plans at least annually;

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.

### PL-4 - Rules of Behavior

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, and security;

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 at least every three years; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge at least annually and when the rules are revised or changed.

***PL-4(1) - Rules of Behavior | Social Media and External Site/application Usage Restriction***

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.

### PL-8 - Security Architecture

a. Develop security architectures for the system that:

   1. Describe the philosophy, requirements, and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. Describe how the architectures are integrated into and support the enterprise architecture; and
   3. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures at least annually or when a significant change occurs to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in the security plans, organizational procedures, and procurements and acquisitions.

### PL-10 - Baseline Selection

Select a control baseline for the system.

### PL-11 - Baseline Tailoring

Tailor the selected control baseline by applying specified tailoring actions.

## PERSONNEL SECURITY (PS)

### PS-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### PS-2 - Position Risk Designation

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 at least every three years.

### PS-3 - Personnel Screening

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

b. Rescreen individuals in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established relative to any regulated data that the position requires access to.

#### *PS-3(3) - Personnel Screening | Information Requiring Special Protective Measures*

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

a. Have valid access authorizations that are demonstrated by assigned official government duties; and

b. Satisfy organization-defined additional personnel screening criteria.

### PS-4 - Personnel Termination

Upon termination of an individual’s employment, agencies must:

a. Disable system access within same day;

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

c. Conduct exit interviews that include a discussion of 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.

### PS-5 - Personnel Transfer

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 transfer or reassignment actions as appropriate following the formal transfer action for all personnel, including contractors within twenty-four (24) hours;

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

d. Notify designated agency personnel, as required within twenty-four (24) hours.

### PS-6 - Access Agreements

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements at least annually; 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 at least annually and any time there is a change to the user's level of access.

### PS-7 - Third-Party Personnel Security

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 the agency of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within organization-defined time period; and

e. Monitor provider compliance with personnel security requirements.

### PS-8 - Personnel Sanctions

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

b. Notify designated agency personnel within same day when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

### PS-9 - Position Descriptions

Incorporate security roles and responsibilities into organizational position descriptions.

## RISK ASSESSMENT (RA)

### RA-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### RA-2 - Security Categorization

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 AO or designated representative reviews and approves the security categorization decision.

### RA-3 - Risk Assessment

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 a risk assessment report;

d. Review risk assessment results at least every three (3) years or when a significant change occurs;

e. Disseminate risk assessment results to designated personnel as defined in the SSP; and

f. Update the risk assessment at least every three (3) years or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security state of the system.

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

a. Assess supply chain risks associated with systems, system components, and system services; and

b. Update the supply chain risk assessment at least every three (3) years or 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.

### RA-5 - Vulnerability Monitoring and Scanning

a. Monitor and scan for vulnerabilities in the system and hosted applications (e.g., operating system/infrastructure, web applications, APIs, databases) monthly and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability scanning 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:

   1. High-risk vulnerabilities mitigated within thirty (30) days from date of discovery;
   2. Moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; and
   3. Low risk vulnerabilities mitigated within one hundred eighty (180) days from date of discovery in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with designated agency personnel to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability scanning tools that include the capability to regularly update the vulnerabilities to be scanned.

***RA-5(2) - Vulnerability Monitoring and Scanning | Update by Frequency / Prior to New Scan / When Identified***

Update the system vulnerabilities to be scanned prior to a new scan, or when new vulnerabilities are identified and reported.

***RA-5(3) - Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage***

Define the breadth and depth of vulnerability scanning coverage.

***RA-5(5) - Vulnerability Monitoring and Scanning | Privileged Access***

Implement privileged access authorization to all components that support authentication for all scans.

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

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

## RA-7 - Risk Response

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

## RA-9 - Criticality Analysis

Identify critical system components and functions by performing a criticality analysis for, system components, or system services and document the analysis in the SSP.

## SYSTEM AND SERVICES ACQUISITION (SA)

### SA-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### SA-2 - Allocation of Resources

a. Determine the high-level information security 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 in organizational program and budgeting documentation.

### SA-3 - System Development Life Cycle (SDLC)

a. Acquire, develop, and manage the system using a SDLC methodology that includes information security considerations that incorporates information security considerations;

b. Define and document information security roles and responsibilities throughout the SDLC;

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

d. Integrate the organizational information security risk management process into SDLC activities.

### SA-4 - Acquisition Process

Include the following requirements, descriptions, and criteria, explicitly or by reference, using State defined standardized contract language in the acquisition contract for the system, system component, or system service:

a. Security functional requirements;

b. Strength of mechanism requirements;

c. Security assurance requirements;

d. Controls needed to satisfy the security requirements;

e. Security documentation requirements;

f. Requirements for protecting security 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 and supply chain risk management; and

i. Acceptance criteria.

#### *SA-4(1) - Acquisition Process | Functional Properties of Controls*

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

#### *SA-4(2) - Acquisition Process | Design and Implementation Information for Controls*

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram.

#### *SA-4(9) - Acquisition Process | Functions, Ports, Protocols and Services in Use*

Require developers of systems, system components, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

#### *SA-4 (10) - Acquisition Process | Use of Approved PIV Products*

Employ only information technology products on the FIPS 201-approved products list for PIV capability implemented within organizational systems for Federal systems where applicable.

### SA-5 - System Documentation

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 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 functions and mechanisms and how to effectively use those functions and mechanisms;
   2. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and recreate selected system documentation if such documentation is essential to the effective implementation and/or operation of security controls; and

d. Distribute documentation to appropriate agency personnel.

### SA-8 - Security Engineering Principles

Apply systems security engineering principles in the specification, design, development, implementation, and modification of the system and system components.

### SA-9 - External System Services

a. Require that providers of external system services comply with organizational security requirements and employ appropriate security controls as defined by State of Oregon Security Standards;

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

c. Employ organization-defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis.

***SA-9(1) - External System Services | Risk Assessments and Organizational Approvals***

a. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

b. Verify that the acquisition or outsourcing of dedicated information security services is approved by organization-defined personnel or roles.

***SA-9(2) - External System Services | Identification of Functions, Ports, Protocols, and Services***

Require providers of all external systems where State information is processed or stored to identify the functions, ports, protocols, and other services required for the use of such service.

***SA-9(5) - External System Services | Processing, Storage, and Service Location***

Restrict the location of information processing, information or data, and system services to organization-defined locations based on organization-defined requirements or conditions.

## SA-10 - Developer Configuration Management

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

a. Perform configuration management during system, component, or service development, implementation, and operation;

b. Document, manage, and control the integrity of changes to the SDLC, including: design; development; system test; unit acceptance test; implementation; operation; and disposal;

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 impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to appropriate personnel as identified in the SSP.

## SA-11 - Developer Testing and Evaluation

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

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

b. Perform unit, integration, system, and regression testing/evaluation in accordance with the Organization’s defined SDLC at organization-defined depth and coverage, to include, at a minimum, the system components to be scanned and the vulnerabilities to be checked;

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.

***SA-11(1) - Developer Testing and Evaluation | Static Code Analysis***

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

***SA-11(2) - Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses***

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

a. Uses the contextual information (e.g., organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels);

b. Employs organization-defined tools and methods;

c. Conducts the modeling and analyses at a breadth and depth of modeling and analyses appropriate for the system; and

d. Produces evidence that meets organization-defined acceptance criteria.

## SA-15 - Development Process, Standards, and Tools

a. Require the developer of the system, system component, or system service to follow a documented development process that:

   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations as needed and as dictated by the current threat posture to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy organization-defined security requirements.

***SA-15(3) - Development Process, Standards, and Tools | Criticality Analysis***

Require the developer of the system, system component, or system service to perform a criticality analysis:

a. During the initiation, acquisition and/or development, implementation, operation and maintenance, and disposal stages of the SDLC; and

b. At a level of rigor sufficient to document and justify critical decisions, including:

   1. Functional statement of need;

2. Feasibility study;
3. Mission and business requirements analysis;
4. Security functional requirements analysis;
5. Inspection and acceptance;
6. System integration;
7. Performance measurement;
8. Configuration management and control;
9. Continuous monitoring; and
10. Hardware and software disposal.

### SA-22 - Unsupported System Components

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:

   1. Extended security support agreement that includes security software patches and firmware updates from an external source for each unsupported component.
   2. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing compensating controls and residual risk acceptance.
   3. Unsupported software without a documented exception must be designated as unauthorized.

## SYSTEM AND COMMUNICATION PROTECTION (SC)

### SC-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### SC-2 - Separation of System and User Functionality

Separate user functionality, including user interface services, from system management functionality.

### SC-4 - Information In Shared System Resources

Prevent unauthorized and unintended information transfer via shared system resources.

### SC-5 - Denial of Service Protection

a. Protect against the effects of denial-of-service (DoS) events including, at a minimum, ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack; and

b. Employ the following controls to achieve the DoS objective:

   1. Configuring systems, firewalls, routers, and other network infrastructure to protect against or limit the effects of DoS attacks; and

   2. Guard against, limit, reduce the susceptibility to, and detect DoS attacks utilizing methods such as:

      i) Configuring systems according to documented and established standards for minimizing the effects of DoS attacks;

      ii) Configuring routers and switches to disable forwarding of packets to broadcast addresses, as applicable;

      iii) Configuring routers and firewalls to filter traffic; and

      iv) Employing increased network capacity and bandwidth combined with service redundancy.

### SC-7 - Boundary Protection

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 logically separated (and physically separated to the extent possible) 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 architecture.

#### *SC-7(3) - Boundary Protection | Access Points*

Limit the number of external network connections to the system.

#### *SC-7(4) - Boundary Protection | External Telecommunications Services*

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

e. Review exceptions to the traffic flow policy at least annually and remove exceptions that are no longer supported by an explicit mission/business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

#### *SC-7(5) - Boundary Protection | Deny by Default / Allow by Exception*

Deny network traffic by default and allow network traffic by exception at managed interfaces.

#### *SC-7(7) - Boundary Protection | Split Tunneling For Remote Devices*

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using a documented and approved procedure consistent with organizational security architecture.

#### *SC-7(8) - Boundary Protection | Route Traffic to Authenticated Proxy Servers*

Route all network traffic to or from the Internet through authenticated proxy servers at managed interfaces.

#### *SC-7(12) - Boundary Protection | Host-based Protection*

Implement Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall at access points and end-user equipment as appropriate.

#### *SC-7(18) - Boundary Protection | Fail Secure*

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

### SC-8 - Transmission Confidentiality and Integrity

Protect the confidentiality and integrity of transmitted information.

#### *SC-8(1) - Transmission Confidentiality and Integrity | Cryptographic Protection*

Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

### SC-10 - Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after no longer than thirty (30) minutes.

### SC-12 - Cryptographic Key Establishment and Management

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with NIST-based guidance for key generation, distribution, storage, access, and destruction.

### SC-13 - Cryptographic Protection

a. Determine the cryptographic uses that comply with applicable laws, statutes, Executive Orders, directives, policies, regulations, standards, and guidance, and

b. Implement the following types of cryptography required for each specified cryptographic use:

   1. At Rest:

      i) Storage-layer encryption (server-side encryption); and

      ii) Application-layer encryption (client-side encryption) where access to the data storage does not permit access to the plain-text data; and

   2. In Transit:

      i) Transport Layer Security (TLS) version 1.2 or later non-deprecated version; and

      ii) Secure Shell family of protocols (SSH).

### SC-15 - Collaborative Computing Devices and Applications

a. Prohibit remote activation of collaborative computing devices and applications; and

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

### SC-17 - Public Key Infrastructure Certificates

a. Issue public key certificates under an EIS approved service provider or issue public key certificates under an agency-documented PKI Certificate Policy (CP) and Certification Practice Statement (CPS); and

b. Include only approved trust anchors in trust stores or certificate stores managed by the Organization.

### SC-18 - Mobile Code

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within systems.

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

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.

### SC-21 - Secure Name / Address Resolution Service (Recursive or Caching Resolver)

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

### SC-22 - Architecture and Provisioning for Name / Address Resolution Service

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

### SC-23 - Session Authenticity

Protect the authenticity of communications sessions.

### SC-28 - Protection of Information at Rest

Protect the confidentiality and integrity of all information at rest.

***SC-28(1) - Protection of Information at Rest | Cryptographic Protection***

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest classified as Level 3 (Restricted) or above.

### SC-39 - Process Isolation

Maintain a separate execution domain for each executing system process.

### SC-45 - System Time Synchronization

Synchronize system clocks within and between systems and system components.

***SC-45(1) - System Time Synchronization | Synchronization with Authoritative Time Source***

a. Compare the internal system clocks at least hourly with an organization-defined authoritative time source; and

b. Synchronize the internal system clocks to the authoritative time source when there is any time difference.

## SYSTEM AND INFORMATION INTEGRITY (SI)

### SI-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### SI-2 - Flaw Remediation

a. Identify, report, and correct system flaws;

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

c. Apply security-relevant software and firmware updates within a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows:

   1. Flaws rated as High and above severity within seven (7) calendar days;
   2. Medium severity within fifteen (15) calendar days; and
   3. All others within thirty (30) calendar days; and

d. Incorporate flaw remediation into organizational configuration management processes.

***SI-2(2) - Flaw Remediation | Automated Flaw Remediation Status***

Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms.

***SA-2(3) - Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions***

a. Measure the time between flaw identification and flaw remediation; and

b. Establish benchmarks for taking corrective actions based on criticality.

### SI-3 - Malicious Code Protection

a. Implement signature based and 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 at least weekly and real-time scans of files from external sources to include endpoints and network entry and exit points as the files are downloaded, opened, or executed ;
   2. Block and quarantine malicious code and alert administrator or defined security personnel near-real-time; and
   3. Send alert to designated agency 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.

### SI-4 - System Monitoring

a. Monitor events to detect:

1. Attacks and indicators of potential attack in accordance with monitoring objectives;
2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system;

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 system monitoring information to personnel or roles designated by the agency as needed to support the agency's continuous monitoring and incident response program.

***SI-4(1) - System Monitoring | System-wide Intrusion Detection System***

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

***SI-4(2) - System Monitoring | Automated Tools for Real-Time Analysis***

Employ automated tools and mechanisms to support near real-time analysis of events.

***SI-4(4) - System Monitoring | Inbound and Outbound Communications Traffic***

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; and

b. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities.

***SI-4(5) - System Monitoring | System Generated Alerts***

Alert appropriate personnel or roles when the following system-generated indications of compromise or potential compromise occur:

a. Presence of malicious code;

b. Unauthorized export of information;

c. Signaling to an external information system;

d. Indicators of potential intrusion;

e. Any incident relevant to the Oregon Consumer Identity Protection Act (OCIPA);

f. Successful phishing attack;

g. DoS attack;

h. Adding an account to or removing an account from any group with administrative privileges; and

i. Unsuccessful login attempts to an account with administrative privileges.

#### *SI-4(16) - System Monitoring | Correlate Monitoring Information*

Correlate information from monitoring tools and mechanisms employed throughout the system.

#### *SI-4(18) - System Monitoring | Analyze Traffic and Covert Exfiltration*

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at organization-defined interior points within the system.

#### *SI-4(23) - System Monitoring | Host-based Devices*

Implement host-based monitoring mechanisms at organization-defined system components.

### SI-5 - Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from EIS/CSS on an ongoing basis. Sources may include, but are not limited to: US-CERT, ICS-CERT, and MS-ISAC;

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

c. Disseminate security alerts, advisories, and directives to appropriate agency personnel, including Agency System Owners; and

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

### SI-6 - Security Function Verification

a. Verify the correct operation of organization-defined security functions;

b. Perform the verification of the functions specified in SI-6a (including upon system startup and/or restart) upon command by user with appropriate privilege; at least monthly;

c. Alert system administrators and security personnel to failed security verification tests; and

d. Take immediate steps to triage and isolate the impacted system or component when anomalies are discovered.

### SI-7 - Software, Firmware, and Information Integrity

a. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information; and

b. Immediately notify designated agency officials when unauthorized changes to the software, firmware, and information are detected.

#### *SI-7(1) - Software, Firmware, and Information Integrity | Integrity Checks*

Perform an integrity check of software, firmware, and information as defined in applicable agency SSPs.

#### *SI-7(7) - Software, Firmware, and Information Integrity | Integration of Detection and Response*

Incorporate the detection of unauthorized security-relevant changes into the organizational incident response capability.

## SI-8 - Spam Protection

a. Employ spam protection mechanisms at system entry and exit points to detect unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

### *SI-8(2) - Spam Protection | Automatic Updates*

Automatically update spam protection mechanisms.

## SI-10 - Information Input Validation

Check the validity of information inputs and verify that inputs match specified definitions for format and content.

## SI-11 - Error Handling

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to authorized personnel or roles as defined in the applicable SSP.

## SI-12 - Information Management and Retention

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.

## SI-16 - Memory Protection

Implement security safeguards to protect the system memory from unauthorized code execution.

## SUPPLY CHAIN RISK MANAGEMENT (SR)

### SR-1 - Policy and Procedures

Refer to the Statewide Information Security Plan for additional details on policies and procedures.

### SR-2 - Supply Chain Risk Management Plan

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 all systems, system components, or system services under configuration management;

b. Review and update the Supply Chain Risk Management (SCRM) Plan every three years or as required, to address threat, organizational or environmental changes; and

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

***SR-2(1) - Supply Chain Risk Management Plan | Establish SCRM Team***

Establish a SCRM Team consisting of personnel, roles, and responsibilities as identified in the SCRM Plan to provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

### SR-3 - Supply Chain Controls and Processes

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of any system or system component, in coordination with personnel or roles as identified in the SCRM Plan;

b. Employ SCRM Controls, as defined in Enterprise policies and Statewide Information and Cybersecurity Standards, and applicable regulatory frameworks, 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; and

c. Document the selected and implemented supply chain processes and controls in the SCRM Plan.

### SR-5 - Acquisition Strategies, Tools, and Methods

Employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks as identified in the SCRM Plan.

### SR-6 - Supplier Assessments and Reviews

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide at least annually.

### SR-8 - Notification Agreements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of:

a. Supply chain compromises;

b. Results of assessments or audits;

c. End-of-support / end-of-life;

d. Major changes in a maintenance organization’s structure or process (for example, physical move to a different location, change in ownership, outsourcing, or changes in personnel);

e. Successful and attempted threat events that may affect Enterprise systems;

f. Available protective or mitigating measures to address identified vulnerabilities; and

g. Any system, service, or component-specific information that affects maintenance or continuity plans.

### SR-10 - Inspection of Systems or Components

Inspect all systems or system components under configuration control upon receipt and before reassignment; and whenever indicators of compromised are reported to detect tampering.

### SR-11 - Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to approved external reporting organizations; personnel or roles as identified in the SCRM Plan.

#### *SR-11(1) - Component Authenticity | Anti-Counterfeit Training*

Train personnel or roles as defined in the SCRM Plan to detect counterfeit system components (including hardware, software, and firmware).

#### *SR-11(2) - Component Authenticity | Configuration Control for Component Service and Repair*

Maintain configuration control over all system components awaiting service or repair and serviced or repaired components awaiting return to service.

### SR-12 - Component Disposal

Dispose of system components using the following techniques and methods:

a. Sanitize all components prior to disposal in accordance with MP-6;

b. Securely dispose of or destroy all components subject to configuration management; and

c. Document all disposals in component inventories.