Statewide
Information Security Plan

Date: 8/1/2018

Contact: Enterprise Security Office

Date	Author	Version	Change Reference
8/1/2018	Vincent.Almberg@oregon.gov	1.0	Initial Version
9/4/2018	Vincent.Almberg@oregon.gov	1.2	Final amendment with State CISO changes

0 Introduction

Information is an asset that, like other business assets, is essential to the agency. Information can exist in many forms. It can be printed or written on paper, stored electronically, sent by post or transmitted using electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately secured.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment. Information security is achieved by implementing controls, such as policies, standards, procedures, organizational structures, and software and hardware functions.

The objectives identified in this plan represent commonly accepted goals of information security management as identified by the International Standards Organization (ISO) 27001:2013 *Information technology – Security Techniques – Information Security Management Systems – Requirements* and ISO 27002:2013 *Information technology - Security techniques - Code of practice for information security management*. While ISO 27001/27003 standards framework is used to organize and articulate the plan, the plan is aligned and informed by NIST guidance and controls. The Center for Internet Security (CIS) Critical Security Controls (CSC) framework is also applied a way to prioritize implementation of this plan throughout the enterprise.

1 Document Scope

The controls documented herein are based on control standards as defined in statewide policy, statewide standards, the NIST Cyber Security Framework (CSF) and the ISO 27001 & ISO 27002 framework. Other frameworks, such as COBIT, ISA, and NIST SP 800-53 have been referenced. The use of established information security/cybersecurity frameworks enables the agency to apply principles and best practices to continuously improve its security posture and address the challenges of emerging threats.

The scope of this document is limited to those areas where the agency maintains sole responsibility. Where shared responsibility exists for systems, networks, applications, and information, those specific responsibilities will be articulated in the Agency Addendums section of this plan.

2 Purpose and Applicability

The purpose of this Information Security Plan is to apply relevant safeguards as identified by statewide policy, statewide standards, the *National Institute of Standards and Technology's* (NIST) *Cybersecurity Framework* (CSF) and *International Standard Organization (ISO) Security Techniques* to State of Oregon agencies and state information, IT systems, networks, and applications.

The quickly changing threat landscape presents increasing risks to the integrity and confidentiality of information. Consequently, vulnerabilities in applications, systems, and networks can negatively impact the availability of information and impede the state government's ability to conduct business.

This plan applies to all Oregon Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 276A.300 and 276A.303, 352.002, 353.020, and OAR 125-800-0020(3)(b) and (4) as they apply to the Oregon State Lottery, Secretary of State, State Treasurer, Public University's and the Attorney General. Applicability is also defined in the Information Security Roles and Responsibilities section of this document – herein referred to as "the agency".

The central guiding principle of the Information Security Plan is to preserve confidentiality, integrity and availability as defined below:

> **Confidentiality:** to keep information from being made available or disclosed to unauthorized individuals, entities, or processes. The practice of maintaining confidentiality ensures that no person or process other than those authorized, can access information.
>
> **Integrity:** to protect data from corruption (modification, loss, replay, reordering, or substitution), either by accident or deliberate tampering. The implementation of integrity safeguards preserves the accuracy and completeness of information and processing methods.
>
> **Availability:** to guarantee that information, data, applications, services, systems and networks are usable when a business process requires them. The preservation of availability ensures that authorized users have access to information and associated assets whenever required.

The State of Oregon Information Security Plan reflects the continuous improvement of security measures and their implementation. This document will be updated and reviewed at a minimum every two years.

2.0.1 Adoption

Compliance to this information security plan, and statewide policies and standards is mandatory. All Executive Branch agencies, as defined above, will use this plan, to manage their information security programs. Pursuant to the ORS 276A.300 and the Statewide Information Security policy, each state agency head is responsible for ensuring his/her agency's compliance with state enterprise security policies, standards, and security initiatives, and with state and federal security regulations. There may be situations in which the legal/regulatory requirements are more stringent than the requirements contained in this plan. In such cases, the agency should ensure compliance with the more stringent legal/regulatory requirements. In areas where controls are required to meet state or federal regulation, the ESO is committed to working in collaboration with the agency to meet the associated ISO or NIST standards through consultative partnership and ESO provided services.

In circumstances where this plan, or portions of this plan, can/will not be implemented, the agency must document the deviations in an agency memorandum. The memorandum will list the deviations in a bulleted format, referencing the paragraph number, reason for the deviation, expected duration, and indicate what

compensating controls have been applied to adequately protect the information. The agency memorandum must be signed by the agency head, retained and submitted to the ESO.

Where the agency needs to append portions of this security plan (e.g. to prescribe agency policies, standards, and procedures that exceed statewide information policies and standards), those portions may be documented in the Agency Addendums section of this plan. (See 18.2.2)

2.1 Target Audience

This document provides guidance and must be made available to all users (as defined in "Information Security Roles and Responsibilities" of this document), and third parties who access state information assets or are authorized to use state information technology. Its aim is to explain the security program, everyone's involvement, and to furnish instructions on the implementation of required security controls.

This plan is also intended to give direction and support for agency defined information security policies, standards and procedures.

While this plan is comprehensive, the supporting documentation (e.g. policies and standards) is also detailed and informative.

2.2 Authority

2.2.1 Leadership and Commitment[1]

The State of Oregon executive management will demonstrate leadership and commitment with respect to the security of its information by:

1) Ensuring the agency's information security policy and information security objectives are established and are compatible with the strategic direction of the statewide plan;
2) Communicating the importance of effective information security and conforming to information security requirements;
3) Directing and supporting persons to contribute to the effectiveness of information security;
4) Promoting continual improvement; and
5) Supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

[1] ISO 27001:2013, para 5.1

3 Terms and Definitions

Asset	Anything that has value to a State of Oregon agency.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
Detect	Develop and implement the appropriate activities to identify the occurrence of an information security event.
Event	An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.
Framework	The implementation tier or lens through which to view the characteristics of an organization's approach to risk – how an organization views information security risk and the processes in place to manage that risk.
Function	A main component of the NIST Cyber Security Framework (CSF). Functions provide the highest level of structure for organizing basic information security activities into categories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Incident	A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action. (see definition of 'Event')
Information Security/ Cybersecurity	Preservation of confidentiality, integrity, and availability of information; in addition, other properties, such as authentication, accountability, non-repudiation, and reliability can also be involved.
Policy	Overall intention and direction as formally expressed by management.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Risk	Combination of the probability of an event and its potential consequences, a measure of the extent to which an entity is threatened by a potential event. A function of the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management	Coordinated activities to direct and control the agency with regard to risk. The process of identifying, assessing, and responding to risk.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or the agency.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by one or more threats.

Must, Should, and Will

The words “must”, “should”, and “will” are used throughout this document. “Must” is used to indicate a requirement. “Should” is used to indicate a recommendation, a desired goal or expected state. “Will” is used to communicate a requirement that will be met in the future.

4 Information Security Program and Risk

4.1 Risk Assessment

Objective: Information security is a business issue. The objective is to identify, assess and take steps to avoid or mitigate risk to agency information assets.

Risk Assessment refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. A risk assessment is critical for the agency to successfully implement and maintain a secure environment. Periodic risk and vulnerability assessments will identify, quantify, and prioritize risks against agency criteria for risk acceptance and objectives. The results will guide and determine appropriate agency action and priorities for managing information security risks and for implementing controls needed to protect information assets. The agency must comply with ORS 276A.300 and provide the OSCIO with assessment results as required.

Table 1 Categorization of Potential Impact to State of Oregon Information and Information Systems

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The agency must conduct risk assessments and include the following steps:

- **Identify the risks**
    a. Identify agency assets and associated information owners;
    b. Identify threats to those assets;
    c. Identify vulnerabilities that might be exploited by the threats; and
    d. Identify impacts that losses of confidentiality, integrity and availability may have on the assets.

- **Analyze and evaluate the risks**
    a. Using Table 1, assess the business impacts on the agency that might result from security failures;
    b. Assess the realistic likelihood of security failures occurring in the light of prevailing threats;
    c. Estimate level of risks; and
    d. Determine whether the risks are acceptable.

- **Identify and evaluate options for the treatment of risk**
    a. Mitigate or reduce the risk: Apply appropriate controls;
    b. Agency Director accepts the residual risk;
    c. Avoid the risks; and
    d. Transfer the associated business risks to other parties.

- **Select control objectives and controls for the treatment of risks**

    It is recognized that no set of controls will achieve complete security. Additional management actions must be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls.

4.2 Establish an information security risk management framework

Objective: Identify the appropriate risk level for the information a State of Oregon agency collects and stores as a function of its service.

Developing an agency information security risk management program, if none exists, will be included in the strategic plan for the agency. The agency must have an agency risk management framework in place that employs an organization-wide or holistic approach to the risk management process. The agency must comply with statewide risk management policy, where one exists, and should leverage available risk management templates for risk plan development and risk determination.

5 Information Security Policies

ORS 276A.300 requires agencies to develop and implement policies, standards, and procedures based on the statewide level policies and standards. This plan and its underlying policies and standards have been developed in compliance with ORS 276A.300. The objective of an information security policy is to provide management direction and support for information security in accordance with business requirements and governing laws and regulations. Information security policies must be approved by the agency executive leadership team, and published and communicated to all employees and relevant external parties. These policies set out the agency's approach to managing information security and align with relevant statewide policies. As stated in the Statewide Information Security Policy, "All State of Oregon personnel, employees, temporary employees, volunteers, and contractors must comply with the State of Oregon information security policies, standards, and procedures." as defined in paragraph 2 of this document.

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Administrative Rules/Policies/Standards/Procedures

Oregon Statute and Administrative Rules:

ORS/OAR Number	Title
ORS 646A.600 through; 646A.628	Oregon Consumer Identity Theft Protection Act
ORS 276A.300	Information Systems Security in Executive Department
ORS 276A.303	Information Systems Security for Secretary of State, State Treasurer and Attorney General
OAR 125-800	State Information Security

Statewide information security policies:

Policy Number	Policy Title
107-001-010	Continuity of Operations Planning
107-004-010	Information Technology Asset Inventory & Management
107-004-050	Information Asset Classification
107-004-051	Controlling Portable and Removable Storage Devices
107-004-052	Information Security Policy
107-004-053	Employee Security
107-004-100	Transporting Information Assets
107-004-110	Acceptable Use of State Information Assets
107-004-120	Information Security Incident Response

107-004-150	Cloud Computing
107-011-050_PR	Sustainable Acquisition and Disposal of Electronic Equipment (e-waste/recovery)
107-011-170	Building Security Access Controls

Statewide information security standards

Standard Number	Standard Title
	Statewide Information Security Standards

5.1.2 Review of the policies for information security

Information security policies must be reviewed at planned intervals of no more than 1 year or when significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Each policy's associated owners and stakeholders have ultimate responsibility for the development, review, and evaluation of their policy. Reviews include assessing opportunities for improvement of information security policies and managing information security in response to changes in threats and risks to business, legal and policy circumstances, and the technical environment.

6 Organization of Information Security

Information security is coordinated across different parts of the agency with relevant roles and job functions. Information security responsibilities will be clearly defined and communicated.

6.1 Internal Organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1.1 Information Security Roles and Responsibilities

Oregon State Chief Information Officer (OSCIO)	Responsible for all State of Oregon IT and computer systems that support statewide goals, as well as developing agency wide IT strategy and policy.
State Chief Information Security Officer (OSCISO)	Responsible for developing and maintaining risk-based, cost-effective information security and privacy-related policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of state agency information systems, to ensure compliance with applicable regulations and statutes. The OSCISO directs Information Security (IS) strategies and policies statewide.
Enterprise Security Office (ESO)	As designated by DAS, leads statewide information security planning and policy development. Conducts security risk and compliance assessments using staff or third party contractors. Responsible to develop, coordinate and maintain the State Incident Response capability. Maintains a forensic analysis capability. Develops information security awareness and training tools. Tracks information security issues and analyzes trends. Identifies and measures information security performance measures. Conducts training, convenes workgroups, conducts workshops, and leads forums to facilitate agency information security activities.
The Agency	All Oregon Executive Branch entities as defined in ORS 174.112, except that "the agency" does not include: the Secretary of State, State Treasurer, and the Attorney General, the Oregon State Lottery, and public universities listed in ORS 352.002.
Agency Head ***(aka Director, Administrator, Superintendent)***	Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. The Agency Head is also responsible for ensuring compliance with statewide security policies, standards, and security initiatives, and with state, federal, and industry regulations.
Agency Executive Leadership	Final approval authority for agency-wide policies. Responsible for ensuring that risk assessments have been conducted in their respective divisions.
Information Security Board	The governing body made up of agency executives and senior management; responsible for providing strategic direction, ensuring

	that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the agency's resources are used responsibly.
Chief Compliance/Audit/ Risk Officer (if applicable)	Responsible for policy and procedure management, compliance monitoring, agency risk management, and investigations.
Agency System Owner	The agency official responsible for procurement, development, integration, modification, or operation and maintenance of an information system. Ensures that system users and support personnel receive the requisite security training. Assists in the identification, implementation, and assessment of information classification, security requirements, and the common security controls.
Agency Information Owner (aka Data Owner)	Management-level individuals (e.g. business owner, department head, division head) that provide input to agency system owners regarding information classification, security requirements, and security controls where their business information resides. Decides who has access to the information and with what types of privileges or access rights, performing periodic classification assessments, and ensures regular reviews to update and manage changes to risk.
Agency Data Custodian (aka Data Steward)	Responsible for assigning access to the information based upon business requirements, need to know, and at the direction of the Agency Information Owner.
Authorizing Official	The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.
Information Systems Auditor (if applicable)	Responsible for the planning, executing, and leading security audits across the agency.
Business Information Security Officer (BISO)	Experienced OSCISO Information Security resource for overseeing Information Security operations within the agency, as well as the overall security posture of systems and controls.
Agency Information System Specialist	Technical agency resource chiefly responsible for administrating access management and information systems, and providing data for security metrics and remediation efforts - which support the agency information security program.
Agency Incident Response Point of Contact	Responsible for communicating with State Incident Response Team and coordinating the agency's actions in response to an information security incident.

Privileged Access User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
User	All employees (including temporary employees), volunteers, their agents, vendors and contractors, including those users affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives and processes.[2] Users are responsible for complying with the provisions of plans, policies, standards, and procedures.

6.1.1.2 Governance

Governance is an essential component for the long-term strategy and direction of an organization with respect to security policies and the risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, business, and information technology management on security issues and acceptable risk levels.

At the statewide level, information security policy development and statewide initiatives are developed collaboratively with agencies. While responsibility for statewide information security has been assigned to the Enterprise Security Office (ESO) by statute and rule, several governance bodies exist to provide advice, guidance, and subject matter expertise in the identification, development, and management of governing policies, guidelines, tools, and initiatives. These governance groups are:

Information Security Council – The Information Security Council (ISC) is chartered to support information security through collaborative efforts to ensure the confidentiality, integrity and availability of the state's information assets. The ISC is the avenue for agencies to participate and assist in the development of strong statewide information security and to provide input for initiatives to meet agency business needs. These efforts include, but are not limited to, identification and development of strategies, policies and initiatives that protect and enhance the security of state information assets. It is the role of the ISC, as the embodiment of information security subject matter expertise in state government, to validate the feasibility of statewide information security initiatives and strategies and make informed, clearly defined and prioritized recommendations to the ESO.

Chief Information Officer Council – The Chief Information Officer Council (CIO Council) is comprised of state and local government chief information officers and information technology leaders. The CIO Council provides a forum for all agencies to collaborate in the management of information resources across state government. The CIO Council advises the State Chief Information Officer and state business leaders on strategic information resource management (IRM) planning, statewide IRM policies, statewide technical architecture and standards, and planning implementation of statewide information technology initiatives.

Agency Heads – The heads of executive branch agencies convene bi-monthly to review information about statewide initiatives and align agency strategies.

Small Agency Heads - The heads of small executive branch agencies convene quarterly to review information about statewide initiatives and align agency strategies.

Administrative Business Services Directors – The DAS Director's Office has chartered this group to provide leadership and feedback on statewide business management opportunities to:

[2] Acceptable Use of State Information Assets, Definitions

1) Provide better efficiency and customer service to state government
2) Share information
3) Identify and provide training and development opportunities
4) Review, discuss and develop work products around the state's business services

Department of Justice – Representatives from the Department of Justice review statewide policies and other documents for legal sufficiency.

In addition, the agency must define and document an information security governance structure tailored to the agency's business needs. The agency governance structure should involve the agency executive leadership. At a minimum, the agency must identify an information security point-of-contact and should identify a representative to the Information Security Council.

An example of responsibilities for an agency governance group are outlined below:

In order to implement and properly maintain a robust information security function, the governance group recognizes the importance of:

- *Understanding information security requirements and the need to establish policy and objectives for information security;*
- *Managing information security risks in the context of overall business risks;*
- *Ensuring all users of agency information assets are aware of their responsibilities in protecting those assets;*
- *Monitoring and reviewing the performance and effectiveness of information security policies and controls; and*
- *Continuous improvement based on assessment, measurement, and changes that affect risk.*

6.1.2 Separation of duties

Roles and responsibilities must be divided so that a single individual, account, or function cannot intentionally or unintentionally subvert a critical process. Care must be taken so that no single person can access, modify or use assets without authorization or detection.

The agency must have written procedures to document the creation, acceptable use, and removal of special access privileges, including high-level privileges (e.g. root access, administrator), system utilities requiring high-level privileges, and privileges that provide access to network devices, operating systems, or software application capabilities (see 9.2.3, Management of Privileged Access Rights, for further guidance). Procedures must include requiring different accounts or different authentication tokens than those used with the individual's regular user account.[3]

As separation of duties, including requiring different accounts for administrative purposes, applies particularly to access management, the agency must document any exception in an agency memorandum. The memorandum will indicate what compensating controls have been applied to adequately protect the information, such as monitoring of activities, audit trails and management supervision. The agency memorandum must be signed by the agency head, retained and submitted to the ESO.[4]

6.1.3 Contact with authorities

The agency must have procedures in place that specify when and who is authorized to contact authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) and how information security incidents will be reported

[3] Statewide Information Security Standards, para 2.1.14
[4] Statewide Information Security Standards, Executive Summary section

in a timely manner (e.g. if it is suspected that laws may have been broken, as in the case of a stolen laptop) (see 16.1.2).

6.1.4 Professional interest groups relating to information security

Professional interest groups (for the purposes of improving a person's knowledge or skills in information security) are defined as an association of individuals or organizations with interest in, or acting in a specific area of knowledge, where members cooperate/work to solve problems, produce solutions, and develop knowledge. Other examples are specialized forums and professional associations. Membership in professional interest groups or forums are encouraged and considered as a means to:

a) improve knowledge about best practices and stay up to date with relevant security information;
b) ensure the understanding of the information security environment is current and complete;
c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
d) gain access to specialist information security advice;
e) share and exchange information about new technologies, products, threats or vulnerabilities;
f) provide suitable liaison points when dealing with information security incidents

Care must be taken that any membership or association does not conflict with State of Oregon ethics laws or specific state agency Code of Conduct.

6.1.5 Information Security in project management

Information security must be integrated into the agency project management methodology to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that:

a) Information security objectives are included in project objectives;
b) An information security risk assessment is conducted at an early stage of the project to identify necessary controls;
c) Information security is part of all phases of the applied project methodology.
d) Information security implications should be addressed and reviewed regularly in all projects.
e) Responsibilities for information security should be defined and allocated to specified roles within all projects.
f) Where projects include the development or modification of information systems, the agency will identify and, where required, ensure system security plans (SSPs) are completed. Systems requiring a SSP include, but are not limited to;
    a. Systems accessible from the internet,
    b. Systems that process, store, or generate Level 3 or higher information,
    c. Systems categorized with a potential impact by the system owner as 'moderate' or 'high' (See Appendix B, Table 1, 14.1, 14.2.9), and
    d. Systems that require oversight. Additionally, where systems require oversight, SSPs will be submitted to the OSCIO for approval.

6.2 Mobile Devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices

6.2.1 Mobile device policy

Mobile devices allow employees to work in multiple locations and to improve their efficiency. But the same features that make these devices desirable make them a security challenge. Mobile devices can easily be lost or stolen, and users may be tempted to download non-secure apps that may contain malware that could be used to steal confidential data.

Note: For the purposes of this section, mobile devices are defined in accordance with the latest revision of NIST Special Publication 800-124. Mobile devices, in this section, do not include laptops, portable devices, or removable media (e.g. cameras, USB drives, portable drives). (See 8.3.1 Management of Portable Devices and Removable Media for additional information.)

Prior to accessing the agency's resources, mobile devices must require a device password/passcode and/or other authentication (e.g. token-based authentication, network-based device authentication, domain authentication and, when applicable, multifactor authentication). Mobile devices should be configured to purge/wipe agency information from the mobile device after 10 consecutive, unsuccessful device logon attempts. Mobile devices that view or store state information must meet the protection and handling minimums defined in the Statewide Information Asset Classification policy and the Statewide Information Security Standards.

When using mobile devices in public places, meeting rooms and other unprotected areas, special care must be taken to ensure that business information is not compromised – such as shoulder surfing or direct visual observation of the device screen.

Mobile devices must also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Devices carrying business information must not be left unattended and, where possible, should be physically locked away. Alternatively, special locks may be used to secure devices.

Training must be arranged for personnel using mobile devices, in order to raise awareness of the additional risks resulting from mobile devices.

Many mobile devices, particularly those that are personally owned (bring your own device, BYOD), are not necessarily trustworthy. Most current mobile devices lack the root of trust features (e.g., trusted platform modules, TPMs) that are increasingly built into laptops and other types of hosts. There is also frequent Jailbreaking and rooting of mobile devices, which means that the built-in restrictions on security, operating system use, etc. have been bypassed. The agency will assume that all mobile devices are untrusted unless the agency has properly secured them and monitors their security continuously while in use with enterprise applications or data.[5] As such, personally owned devices must not be connected to computers, state networks (including remotely used computers) or other equipment without approval of the agency prior to connection.[6] Approval must be documented and retained. (See also 8.3.1)

Where regulated data exists (e.g. PII, FTI, CJI, HIPAA, PCI, etc.), the agency must comply with all federal and state requirements prior to approving mobile device access to agency resources.

6.2.2 Remote access

Remote access refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as "telecommuting", "flexible workplace", "remote work", and "virtual work" environments.

Access to state agency networks from remote locations is not allowed except through the use of agency-approved and agency-provided remote access systems or software.[7] At a minimum, all remote access must comply with State of Oregon information security standards. These standards include documenting all remote access approvals and requiring computers that are connected directly to the agency's internal network via remote access to use the most up-to-date anti-virus software and operating system and application patches. Additional protection of state agency assets for remote users should also be addressed and identified (e.g. lockable filing cabinets, clear desk

[5] NIST Special Publication 800-124r1, para 2.2.2
[6] Acceptable Use of Information Assets, para III
[7] Acceptable Use of Information Assets, para III

policy, access to agency computers, and secure communications between the remote site, agency offices and network resources). All remote users must be familiar with statewide remote access standards.[8]

[8] Statewide Information Security Standards, para 2.6

7 Human Resources Security

7.1 Prior to employment

Objective: To ensure that users understand their responsibilities and are suitable for the roles for which they are considered.

The agency will provide expectations on employees' responsibilities to help employees understand their responsibilities to reduce the risk of theft, fraud or misuse. Security responsibilities will be addressed prior to employment in job announcements, position descriptions, and contracts with associated terms and conditions of employment. Access to information will be based on business need and conform to the principle of least privilege. Managers, working together with IT Management and Information Owners, are responsible to ensure security is applied throughout an individual's employment with the agency (see 9.2.2).

7.1.1 Screening

The agency will ensure that persons employed have not engaged in criminal behavior that is incompatible with their duties and the mission of the agency. To achieve this goal, and where the authority exists to conduct criminal records checks exist, the agency will include a notice in hiring announcements that background checks will be conducted on potential candidates. As a condition of employment, applicants must sign an authorization form allowing the agency to conduct a criminal background check. Human Resources will partner with the agency's procurement and contracting section and the relevant managers to ensure all contractors assigned to work on behalf of the agency require criminal background checks. Where regulated data exists (e.g. PII, FTI, CJI, HIPAA, PCI, etc.), the agency will comply with all federal and state requirements prior to approving access to state systems.

The agency will add security aspects to all employees' position descriptions and performance evaluations.

7.1.2 Terms and conditions of employment

The agency will communicate to all new hires, during the pre-employment or new hire process, roles and responsibilities as they pertain to information security.

The responsibility for users will reflect the organization's policies for information security. This includes, but is not limited to:

a) Users given access to confidential information may be required to sign a confidentiality or non-disclosure agreement prior to being given access to information or information processing areas (see 13.2.4);
b) Users legal responsibility and rights, e.g. regarding copyright laws or data protection (see 18.1.2 and 18.1.4);
c) Users responsibility regarding the classification of information and management of information assets, information processing facilities and information services;
d) User responsibility for handling information received from other companies or external parties;
e) Enforcement actions taken if the user disregards the organization's security requirements (see 7.2.3).
f) User responsibility for complying with statewide policy, plans, and standards.

7.2 During employment

Objective: To ensure that users are aware of and fulfill their information security responsibilities.

7.2.1 Management responsibilities

Management responsibilities include ensuring that users:[9]

a) Are properly briefed on their information security roles and responsibilities prior to being granted access to information or information systems;
b) Are provided with guidelines explaining information security expectations of their role within the organization;
c) Have received training on acceptable use, understand their responsibilities and follow the Acceptable Use Policy (see 8.1.3);
d) Receive a copy of, or hyperlink to, all statewide and agency information security policies;
e) Know the importance of protecting information assets that can be exposed during voice/data transmissions or with the loss or theft of a portable device;
f) Are trained on information security relevant to their roles and responsibilities within the organization (see 7.2.2);
g) Comply with the terms and conditions of employment;
h) Have or obtained the appropriate information security skills and qualifications and receive approved education on a regular basis;
i) Are informed of the anonymous reporting channel to report violations of information security policies and procedures ("whistle blowing").[10]

Management must demonstrate support of information security policies, procedures and controls, and act as role models.

7.2.2 Information security awareness, education and training

All users, must receive appropriate awareness training and updates on information security policies, plans, standards and procedures as is relevant for their job function. The agency must conduct and document the completion of annual information security awareness training for all users.[11]

As part of the statewide awareness and training program, users will be trained in their responsibilities to ensure unattended equipment has appropriate protection, as well as the need to protect sensitive information where it is processed or viewed, printed, copied, scanned, and faxed, the use of passwords, how different classification levels determine information assets are handled, and when and how information is transported and disposed.

Clean desk practices should be maintained to protect level-3 and level-4 information from view at all times. Access to password-protected systems must automatically lock workstation screens after a defined period of inactivity[12]. All users are required to lock workstation screens when leaving their work area and not to rely on the automated system settings[13]. All remote users must be trained on the required protections for remote access. (See 6.2.2)

The agency must ensure compliance with information security policies, plans and standards, and determine the effectiveness of information security awareness, and training efforts, by conducting periodic random audits that include spot checks on doors and cabinets, password compliance, clean desk audits, and completion of information security awareness and training requirements upon initial hire and annually thereafter.

The agency should develop additional training on various security-related topics to meet regulatory requirements and/or enhance employee's information security awareness training. Examples of additional information security training include, but are not limited to:

[9] Statewide Acceptable Use of State Information Assets, Procedures
[10] Managing Improper Governmental Conduct Policy, 50-090-01
[11] Senate Bill 90, Section 2(2)(c)
[12] Statewide Information Security Standards, para 2.1.17
[13] Statewide Information Security Standards, para 2.1.16

- Acceptable Use of Information Systems policy
  - Acceptable Use of Information Systems standard,
  - Clean Desk standard,
  - Removable Storage standard
- Incident Response
  - Security Breach,
  - Lost Portable Device
- Information Asset Classification and Transporting Information Assets policies,
- Password Management policy,
- Physical Security

7.2.3 Disciplinary process

Users that are found to have violated information security policies, plans, standards, and procedures may be subject to disciplinary action, up to and including termination of employment or contract.[14]

7.3 Termination and change of employment

Objective: To protect state agency interests when staff change positions or terminate employment.

7.3.1 Termination or change of employment responsibilities

The agency is responsible for granting and monitoring users' access only to systems and information required to do their work, and for revoking user access in a timely manner. The agency must have procedures for the identification and removal of unneeded access when users change positions or leave the agency. Upon termination, procedures must be followed to immediately remove or suspend the access rights to information and assets associated with information processing facilities and services. (See 9.2.5 & 9.2.6)

The agency must regularly audit and compare users listed on the state's personnel database to ensure that terminated employees have network access removed.

[14] Acceptable Use of State Information Assets

8 Asset Management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protective controls.

8.1.1 Inventory of Assets

All agency information assets must be identified and inventoried. The Statewide Information Asset Classification policy and the Information Technology Asset Inventory & Management policy require the agency to identify, classify, and manage information assets during their lifecycle from creation to disposal. The responsibility and scope of information asset inventory efforts is for information and system owners to identify and classify information assets, which includes hardware, software, and information in both paper and electronic formats. Proper levels of protection will be implemented to protect assets relative to their classification. The agency must have written hardware and software asset inventory procedures, which detail the processes, responsibilities, and technology for tracking and managing approved and unapproved hardware and software assets. The agency should use the latest version of the Center for Internet Security (CIS) controls framework for inventory and control guidance.

8.1.2 Ownership of assets

All information will have an information owner, or owners, established within the agency's lines of business. Likewise, all systems will have a system owner, or owners. Owners can be individuals or groups of individuals as best meets the business model of the agency. Owners of assets, whether information or systems, have responsibility for assigning risk classifications and for approving appropriate controls or permissions.

Owner(s) will be responsible to:

a) Ensure that assets are inventoried;
b) Ensure that assets are appropriately classified and protected;
c) Define and periodically review access restrictions and classifications to assets, taking into account applicable access control policies;
d) Ensure proper handling when the asset is deleted or destroyed.

8.1.3 Acceptable use of assets

All users having access to agency assets must be trained on the Statewide Acceptable Use of Information Systems policy and the agency Acceptable Use of Information Systems policy, where one exists, and acknowledge understanding and acceptance of compliance, on initial hire and an annual basis (see 9.2.1, 9.2.2).

8.1.4 Return of assets

All users must return all agency assets in their possession upon termination of employment, contract or agreement. In cases where a user uses their own personal equipment (See 6.2.1, 8.3.1, and 9.1.2), procedures must be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see 11.2.7).

8.2 Information classification

Objective: To ensure that information receives the level of protection appropriate to its importance.

8.2.1 Classification of information

The Statewide Information Asset Classification policy outlines principles for how state agency information, or data, must be managed from creation to utilization, and disposal. To ensure information receives an appropriate level of protection, information will be classified to indicate the sensitivity and expected degree of protection for

handling. The State of Oregon uses four levels of information asset classification identified in the DAS Information Asset Classification policy.

- **Level 1, Published**
- **Level 2, Limited**
- **Level 3, Restricted**
- **Level 4, Critical**

The agency must use the appropriate level of protection for the assigned level of risk for all information assets. For example, when the highest level of protection is required (Level 4 - Critical information), the information must be protected according to Statewide Information Security Standards (e.g. by a double set of physical protection (for example in a locked file cabinet in a locked room), encryption and password control). (See 11.2.1)

Information received from another agency must be maintained according to the classification assigned by the owner agency, as stated in established agency agreements (e.g. inter-agency agreement, access agreement, data use agreement, etc.).

Owners of information assets, as defined in the Statewide Information Asset Classification policy, have responsibility for assigning the risk classification of those assets and approving appropriate controls. All users must be provided a copy of, or link to, the Statewide Information Asset Classification policy and must comply with the information classification, transmission, storage, processing, and retention requirements for all state agency information. If users have any questions concerning the protection or handling of information assets, they should contact their immediate supervisor, the agency records officer or an information security officer. (See 8.1.2)

8.2.2 Labeling of information

The key to effective labeling is ensuring that a person with access to the information is aware of its classification and what restrictions exist in the release or handling of the information.[15] At a minimum, all Level 2 or higher information, including but not limited to paper, electronic, and media, must be labeled and encrypted appropriate to the classification. Labelling will reflect the classification scheme established in paragraph 8.2.1. Labels must be easily recognizable and comply with the "Labeling Limited, Restricted, or Critical Information" section of the statewide Information Asset Classification policy.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of portable devices and removable media

Information assets, which include information residing on removable storage devices, must be physically secured in a manner that protects sensitive information from unauthorized or accidental disclosure, modification, or loss. All users will be familiar with the statewide standards and agency approval procedures prior to using removable storage devices with the state agency computing environment, for example: portable devices must not be left unattended in uncontrolled access areas.[16]

[15] Statewide Information Asset Classification
[16] Statewide Information Security Standards, para 1.5.1

Note: Unlike paragraph 6.2.1, for the purposes of this section, portable devices and removable media include mobile devices (as defined in accordance with the latest revision of NIST Special Publication 800-124), as well as, but not limited to, cameras, USB Drives, and portable drives.

If the agency chooses to allow personally owned portable devices and removable media to connect to state owned equipment, the agency must have a written procedure by which users are granted approval. All users must be granted approval, in accordance with the agency written procedure and in writing, prior to attaching any personally owned portable devices and removable media to state equipment.[17] (See 6.2.1 & 8.2.2)

The "Asset Management" and "Handling of Information Assets" sections of the Statewide Information Security Standards defines the base levels of protection of the agency's information assets. The agency must take measures to encrypt Level 3 and Level 4 data on portable devices[18] and protect it with a password that meets the minimum statewide information security standard password requirements[19]. If portable drive or data encryption is not possible, then the agency must provide physical control guidance to ensure the security of the data. (See 8.3.3) Management may institute more stringent levels of protection based upon business needs.

Information owners must develop procedures specific to their business area to monitor the location and the type of information stored on portable devices.

8.3.2 Disposal of information or media

When sensitive information or equipment containing agency information reaches retention or end-of-life, appropriate disposal procedures must be followed. All electronic, paper and physically recorded information assets must be disposed of in a manner consistent with the information asset classification and comply with established State of Oregon archive laws, rules and regulations. For disposal of electronic equipment, refer to Statewide DAS Procedure 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E- Waste/Recovery Policy).

8.3.3 Transporting information assets

The Statewide Transporting Information Assets policy outlines necessary protections for transporting information assets including, but not limited to, the use of reliable carriers and ensuring security language is incorporated into use agreements; ensuring employees who carry sensitive information follow information handling requirements; packaging to protect the contents; labeling that is clear on both the inside and outside of the package; maintaining a chain of custody; and using other risk management techniques such as using lockable storage containers, tamper evident packaging, and encryption technologies where appropriate.

[17] Statewide Information Security Standards
[18] Statewide Information Security Standards
[19] Statewide Information Security Standards

9 Access Control

9.1 Business requirement of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access management

Access to information, information systems, and information processing facilities are controlled according to business needs and information security requirements. The agency will comply with the Statewide Information Security Standards. Formal policies, standards, and procedures provide guidance to controlling access to information, information systems, and services and to help prevent unauthorized access. Where regulated data exists (e.g. PII, FTI, CJI, HIPAA, PCI, etc.), the agency is expected comply with all federal and state requirements prior to approving access to state systems.

9.1.2 Access to networks and network services

Devices connected to the agency internal network must comply with established statewide policies and standards. Non-state agency owned portable devices are prohibited from connecting to state networks until the agency grants and documents approval to attach the equipment through an exception and approval process. (See 6.2.1, 8.3.1, 13.1.2)

9.2 User access management

Objective: To ensure authorized access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

The State of Oregon reserves, and intends to exercise, all rights relating to all information assets. The agency is responsible for granting and monitoring users' access only to systems and information required to do their work, and for revoking user access in a timely manner. The agency may withdraw permission for any or all use of its systems at any time without cause or explanation.[20]

A formal user registration and de-registration procedure must be documented and implemented to enable assignment, or revocation, of access rights. User IDs and passwords must comply with the Statewide Information Security Standards. The process for managing user IDs will ensure the use of unique user IDs that enable users to be linked to and held responsible for their actions. User IDs will be immediately disabled or removed for users who have left the organization (see 9.2.6);

Shared accounts (e.g. service accounts, network equipment, and multi-function printer administration) are only permitted if approved, and procedures and processes in place to ensure authorization and accountability. To ease the process of authorization and accountability, the agency should employ an enterprise password management solution to assist in the auditing, storing, and managing of shared account events – where shared accounts can be used without disclosing passwords in plain-text.

9.2.2 User access provisioning

The provisioning process for assigning, modifying, or revoking access rights granted to users will follow agency policies, standards, and procedures, which will include obtaining authorization from the information owner (see 8.1.2).

User access provisioning will ensure that, at a minimum, the following access controls are enforced:

[20] Statewide Acceptable Use of State Information Assets

1) Separation of duties (see 6.1.2),
2) Ensuring that access rights are not activated before authorization procedures are completed (e.g. service providers),
3) Adapting access rights of users who have changed roles or jobs, and
4) Immediately removing or blocking access rights of users who have left the organization (see 9.2.5).

Assignment of privileged access must be based on job classification and function (see 9.2.3).

9.2.3 Management of privileged access rights

Privileged roles (or special access privileges) are defined as roles assigned that allow individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.[21] Additionally, privileged users, including super users, are typically described as system administrators for various types of commercial off-the-shelf operating systems.[22]

The allocation of privileged access rights must be controlled through a formal authorization process. Privileged access rights must be allocated to users on an "as needed" basis, must not be granted until the authorization process is complete, and must be reviewed regularly (see 9.2.5). In accordance with the Statewide Information Security Standards[23], the agency must have written procedures to manage privileged access accounts. Privileged accounts must only be used for administrative activities and not internet browsing, reading e-mail, or composing documents. The agency should use the latest version of the Center for Internet Security (CIS) controls framework for controlled use of administrative privileges guidance.

All devices, systems, and software must log the activities of privileged users. Logs recording privileged user activities must be descriptive, specific and granular. Additionally, privileged user activity must be monitored, and specific behaviors alerted, for example, when a privileged user attempts to increase privileges, when a privileged user attempts to modify logs, and when a privileged user attempts to create another account, or assign privileges.

9.2.4 Management of account logon information of users

All users must abide by the Statewide Information Security Standards, and must manage passwords or pass phrases to meet or surpass minimum standards for passwords. Statewide Information Security Standards state that the construction and specifications of a password must be defined in agency policy and must be of a complexity consistent with the information classification level the user has access to.[24] Requirements in this standard applies to all users and passwords used to access state agency systems, databases, and applications. Users of state information systems must be trained to not reuse their state account passwords for any other purpose.[25]

Procedures must be established to verify the identity of a user prior to providing new, replacement or temporary passwords or account information. Temporary passwords must be given to users in a secure manner and unique to an individual and should not be guessable.

Default vendor authentication information must be altered following installation of systems or software.

[21] NIST SP 800-53r4, AC-2(7)
[22] NIST SP 800-53r4, AC-6(5)
[23] Statewide Information Security Standards
[24] Statewide Information Security Standards
[25] Statewide Information Security Standards

9.2.5 Review of user access

User access (e.g. privileged access rights, security group membership, email distribution lists, systems access, facility access) must be reviewed by the users manager, working together with IT management and Information Owners, upon initial hire, during annual reviews, changes in job position (such as promotion or demotion), or transfers to another division or section within the agency.[26] (See 7.3.1)

9.2.6 Removal or adjustment of access rights

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services must be immediately removed or suspended. If a transferring or departing employee or external party user has known passwords for user IDs remaining active, procedures must be followed that they be changed upon change of employment, termination of contract or agreement, or termination from the agency. (See 7.3.1 & 9.2.5)

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of account logon information

Users must keep secret authentication information (e.g. usernames and passwords) confidential, ensuring that it is not divulged to any other parties, including supervisors, family members, or co-workers.[27] Additionally, users will avoid keeping a record of secret authentication information on paper or device, unless this information can be stored securely (e.g. locked cabinet or encrypted device with security enabled). Users will understand and comply with the statewide authentication standard.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Access to information on agency information and information assets must be restricted based upon their various levels of sensitivity and value. The Statewide Information Asset Classification policy states that the agency will identify and classify all agency information and information assets. The agency must use the classification schema included in the Statewide Information Asset Classification policy and each information asset classification will have a set or range of controls, designed the appropriate level of protection of the information commensurate with the value of the information in that classification. The agency must have procedures for identifying, classifying and protecting information assets within the agency's lines of business.

9.4.2 Secure logon procedures

Passwords must be masked on login to all information systems so the password cannot be read off of the screen and authentication must occur through encrypted channels, using methods such as Kerberos, SSH, SSL, etc. Additionally, logon controls must be implemented to protect information systems from brute force password guessing attacks and commensurate with the associated risk to the information system and information.[28]

[26] ISO 27002:2013 9.2.3, 9.2.5
[27] Statewide Information Security Standards, para 2.1.2
[28] Statewide Information Security Standards, para 2.1

9.4.3 Password management system

The agency must utilize a password management system, such as Active Directory, to manage authentication, user, device, and group management, and support for role based access for applications.[29] Passwords not managed by a password management system (e.g. stored on servers or clients), must be stored with password protection and encryption.[30]

9.4.4 Use of privileged utility programs

The State of Oregon employs the principle of least privilege, allowing only authorized access for users which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The agency must manage privilege access (see 9.2.3), audit the execution of privileged functions, and prohibit non-privileged users from executing privileged functions. Additionally, users that do not possess appropriate authorizations to manage privileged utility programs are prohibited from disabling, circumventing or altering implemented security safeguards on agency systems (e.g. firewalls, malicious code protection mechanisms).[31]

9.4.5 Access control to program source code

Any changes to the hardware, software, and/or firmware components of agency systems can potentially have significant effects on the overall security of the systems. Therefore, the agency permits only qualified and authorized individuals to access agency systems for initiating changes, including upgrades and modifications. Access to operating system, source code, and operational or production application software/program directories, locations, and configuration files must be managed, limiting access to authorized individuals.[32] Access rights must be granted by the system or information owner, or his/her delegate. (See 9.2.2) Back-up copies of source code must be protected in the manner required by the Statewide Information Asset Classification policy and Statewide Information Security Standard.

[29] Statewide Information Security Standards, para 2.2.4
[30] Statewide Information Security Standards, para 2.1.12
[31] NIST SP 800-53r4, AC-6
[32] Statewide Information Security Standards, para 7.1.1

10 Encryption

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, and integrity of information.

10.1.1 Policy on the use of encryption

Cryptography or the encryption of data and communications, is an important tool for information security. All security controls take some commitment and effort to implement, and encryption is no exception. Media and transport encryption technologies exist to help facilitate employee compliance with the above mentioned policies.

The agency will adhere to the Statewide Information Security Standards for the protection (which includes encryption) and handling of information in storage and transit.

When data is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption that complies with Statewide Security Standards.

Encryption shall not be required if the transmission medium meets all of the following requirements:

1. The agency owns, operates, manages, or protects the medium.
2. Medium terminates within physically secure locations at both ends with no interconnections between.
3. Physical access to the medium is solely controlled by the agency.
4. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.

Examples:

- A campus is completely owned and controlled by the agency – If line-of-sight between buildings exists where a cable is buried, encryption is not required.
- A multi-story building is completely owned and controlled by the agency – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by the agency and other non-agency tenants – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

All systems that store classification level 3, or higher data, must be configured to use full-disk encryption technologies.

All users will be familiar and comply with the Statewide Information Asset Classification policy and the encryption and cryptography standards described in the Statewide Information Security Standards document (see 7.2.2, 8.1.2, 8.1.3). If users have any questions concerning the protection or handling of information assets, they should contact their immediate supervisor, the agency records officer or an information security officer.

10.1.2 Key management

The management of cryptographic keys is essential to the effective use of encryption. In all cases where encryption is used, cryptography and key management will comply with Statewide Information Security Standards. Secret and private keys require protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys will be physically protected.[33] Key management or escrow processes

[33] ISO 27002:2013, 10.1.2

must be used when using a key-based data encryption system. In addition, encryption keys suspected of having been compromised must be replaced immediately.[34]

[34] Statewide Information Security Standards, para 3.1.2 & 3.1.3

11 Physical and Environmental Security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities

11.1.1 Physical security perimeter

The agency will comply with the Physical and Environmental Security Standards[35] and ensuring, through documented agreements that all third parties acting on their behalf comply. In circumstances where the standards can/will not be implemented, the agency must document the deviations in an agency memorandum and indicate what compensating controls have been applied to adequately protect information. The agency memorandum must be signed by the agency head, retained and submitted to the ESO.[36]

11.1.2 Physical entry controls

All facilities must have, at a minimum, a single physical security control protecting it from unauthorized access, damage, or interference. All facilities that process or store information classified at level 3 or 4 must have multiple layers of physical security controls.[37] Access to facilities is removed when staff are no longer employed with the agency (see 9.2.6). Where physical entry controls are needed, the Statewide Building Security Access Controls policy provides guidance on mechanical and electronic controls where facilities are owned, managed or leased by DAS for the agency.

Managers, Security Personnel and Human Resources may occasionally make requests to have a particular individual's access audited.

11.1.3 Securing offices, rooms and facilities

The objective of physical and environmental security is to prevent unauthorized physical access, damage, theft, compromise, and interference to the agency's information and facilities. Locations housing critical or sensitive information or information assets must be secured with appropriate security barriers and entry controls. Secure areas must be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Data centers, server rooms, and wiring closets must have strict access controls with physical locking mechanisms and must comply with the Statewide Information Security Physical and Environmental Security Standards.[38]

11.1.4 Protecting against external and environmental threats

Information system backups must be stored in a secured, geographically separated location in accordance with the agency business continuity and disaster recovery plans. If backups are stored offsite using a third-party vendor, vendor practices must comply with state policies on information protection and must meet these standards.[39] The agency will establish an alternate processing site including any necessary agreements to permit the transfer and resumption of its essential business functions when the primary processing capabilities are unavailable.[40] The agency must identify information assets that require power equipment and power cabling to protect from power outage or power damage and destruction. Additionally, the agency must identify any information systems that

[35] Statewide Information Security Standards, para 4.1
[36] Statewide Information Security Standards, Executive Summary
[37] Statewide Information Security Standards, para 4.1.2
[38] Statewide Information Security Standards, para 4.1
[39] Statewide Information Security Standards, para 5.5.3
[40] NIST SP 800-53r4, CP-7

require additional protection measures that include cameras, maintaining fire suppression and detection devices, temperature and humidity controls.

11.1.5 Working in secure areas

The agency may prohibit individuals from bringing portable devices, cell phones, or digital cameras into specific areas within its facilities where assets contain confidential or sensitive information or sensitive conversations are taking place.

11.1.6 Delivery and loading areas

Delivery and loading areas and other points where unauthorized persons could enter the premises must be controlled to avoid unauthorized access. Access to delivery and loading areas from outside of state agency buildings is restricted to identified and authorized personnel. This includes securing external doors of a delivery and loading area when the internal doors are opened and keeping the delivery and loading area designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of state agency buildings.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

The agency will have controls to minimize the risk of potential physical and environmental threats (e.g. theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, and vandalism). Environmental conditions should be monitored for conditions which could adversely affect the operation of its information processing facilities. Guidelines will be established for eating, drinking and smoking in proximity to state owned equipment and facilities.

11.2.2 Supporting utilities

In accordance with business continuity and disaster recovery plans, the agency will identify and plan for alternate telecommunications services (e.g. data and voice). Planning should include necessary agreements to permit the resumption of its essential business operations when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.[41] In addition, consideration should be made for emergency lighting and that emergency communications are provided.

11.2.3 Cabling security

Physical security safeguards applied to transmission lines help to prevent accidental damage, disruption, and physical tampering. The agency must control physical access to its controlled and restricted areas.

11.2.4 Equipment maintenance

The agency must specify information assets that result in increased risk to its organizational operations, individuals, or other organizations and have appropriate contracts in place for maintenance support and/or spare parts to meet its recovery time objective. The agency will schedule, perform, document, and review records of maintenance and repairs on major information assets in accordance with manufacturer or vendor specifications and will approve and monitor all maintenance activities, whether performed on site or remotely.

11.2.5 Removal of assets

[41] NIST SP 800-53r4, CP-8

The agency must require explicit approval from the information owner for the removal of any asset containing level 3 information or higher for off-site maintenance or repairs. Users and third-party partners who have authority to permit off-site removal of assets will be identified. Physical and technical safeguards for media (diskettes, removable drives, flash drives, compact disks, and paper) will be commensurate with the information classification level residing on the media. Safeguards to protect media during transport include locked containers and cryptography. The agency must use appropriate security controls as defined in the Statewide Transporting Information Assets policy. (See 8.3.3)

11.2.6 Security of equipment and assets off-premises

When using portable devices, special care must be taken to ensure that information is not compromised, such as, when using portable devices in public places, meeting rooms and other unprotected areas. Portable devices must not be left unattended in uncontrolled areas.[42] Portable devices must be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Training will be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented. Additional protection of state agency assets for remote users should also be addressed and identified (e.g. lockable filing cabinets, clear desk policy, access to agency computers, and secure communications between the remote site and state agency offices).

11.2.7 Secure disposal or re-use of equipment

All information technology equipment that is no longer needed is processed through the state's salvage operation which follows secure destruction practices. Equipment containing storage media must be checked to ensure that sensitive information and licensed software have been removed or securely overwritten prior to disposal in compliance with statewide policies.

11.2.8 Unattended user equipment

Devices carrying important, sensitive or critical business information must not be left unattended and, where possible, should be physically locked away. Training should be arranged for personnel using mobile devices to raise awareness of the additional risks resulting from this way of working and of controls that should be implemented.

11.2.9 Clean desk policy

Clean desk practices for level 3 or higher information (which include both paper and electronic formats) and removable storage devices must be enforced in all areas. A screen lock policy, as defined in the Statewide Information Security Standards, must be implemented to password-protect information systems.[43] In addition, physical media and paperwork with sensitive information must be protected in accordance with Statewide Information Security Handling of Information Asset Standards.[44] The agency will require users to lock their screen at any time when leaving their work area and be reminded not to rely on automated system settings. Steps must be taken to restrict access to operating systems to only authorized users. Protection must be required and commensurate with risks when using teleworking facilities.

[42] Statewide Information Security Standard, para 1.5.1
[43] Statewide Information Security Standards, para 2.1.17
[44] Statewide Information Security Standards, para 1.2

12 Operations Security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1a Concept of Operations

The agency must develop a Concept of Operations (CONOPS) document for how the organization intends to operate from the IT security standpoint. CONOPS clearly and concisely expresses management's goals and objectives in meeting information security requirements, its partnership with the ESO and how it will capitalize on ESO and ETS shared services, its operational processes with inherent information security responsibilities, and how the program will be sustained using available resources.

12.1.1b Documented operating procedures

Documented procedures must be prepared for operational activities and made available to all users who need them. In addition to procedures noted as required within this plan, other operating procedures will include, but are not limited to: a) the installation and configuration of systems; b) backups; c) support and escalation contacts, including external support contacts in the event of unexpected operational or technical difficulties; monitoring procedures; and server restart and recovery procedures for use in the event of a system failure.

12.1.2 Change Management/Configuration change control

Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications.

The practice of configuration change control includes changes to baseline configurations for components and configuration items of systems; changes to configuration settings for component products; unscheduled or unauthorized changes; and changes to remediate vulnerabilities. This process will include planning and testing of changes, assessment of potential security and business impacts, formal approval procedures for proposed changes, communication of change to all relevant persons, fallback or back-out procedures, and an audit log containing all relevant information. Appropriate processes and levels of review are applied to each type of change commensurate with the potential to disrupt agency operations. An after-action review meeting should be conducted to discuss and document observations made during the course of the change and considerations for enhancement of the change control process.

All changes to information systems or services will follow the CM family of controls in the latest revision of NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations" and the Statewide Information System Development Lifecycle Standard to ensure appropriate planning and execution.[45]

Changes should follow ITIL change management or NIST 800-128 configuration management practices and be categorized (e.g. Standard Change, Minor Change, Major/Significant Change, or Emergency Change). Provisions for an Emergency Change procedure must be established to enable quick and controlled implementation of changes needed to resolve an incident.

In addition, the agency must have written configuration management procedures which detail the processes, responsibilities, and technology for managing the software security configurations of laptops, servers, and

[45] Statewide Information Security Standards, para 7.1.2

workstations. These procedures will be used in enforcing a rigorous configuration management and change control process. Procedures will include:

1) Developing, documenting, and maintaining a current baseline configuration of agency information systems.
2) Employing integrity verification tools (e.g. Microsoft System Center Configuration Manager, Splunk, or Nessus SecurityCenter) to detect unauthorized changes to organization-defined software, firmware, and information.
3) Documenting and implementing configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.
4) Monitoring and controlling changes to the configuration settings in accordance with organizational policies and procedures.

12.1.3 Capacity management

Capacity planning is considered a part of operations and can be attributed to different areas in the information system, such as disk space, bandwidth, and database space. At a minimum, the agency will monitor and forecast capacity on all systems identified, by the owner, as critical.

12.1.4 Separation of development, testing and production environments

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. Additionally, where development and testing personnel have access to the production system and its information, confidentiality is compromised and may be threatened. Other than in exceptional circumstances, testing will not be done on production systems. Where Level 3, or higher, data or systems categorized 'moderate' or 'high', based upon a Business Impact Assessment, production, development, and testing environments must be segregated from one another, e.g. network segmentation, VLANS.[46]

In circumstances where the separation of development, testing and production environments can/will not be implemented, the agency must document the deviations in an agency memorandum and indicate what compensating controls have been applied to adequately protect the information. The agency memorandum must be signed by the agency head, retained and submitted to the ESO.

Level 3, or higher, agency information must not be copied into testing or development environment. Where exceptions exist for allowing PII or otherwise confidential information to be used for testing purposes, the agency must document the business reason, compensating controls, and exception be approved, in writing, by the Agency Head. The documented compensating controls must be at least be equivalent to the controls provided for the production system. (See 14.3.1 for additional guidance)

12.2 Protection from malware and endpoint management

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Precautions must be taken to prevent and detect the introduction of malicious code and unauthorized mobile code and to protect the integrity of software and information. Each computer, herein defined as an endpoint, is responsible for its own security. Agency endpoints must have updated endpoint security software installed

[46] Statewide Information Security Standards, para 6.1.9

upon them and be managed with on-going updates and reporting. Endpoint security software includes, but is not limited to:

- Malware removal;
- Anti-spyware protection;
- Ingress/Egress firewall;
- Host-based IPS/IDS sensors and warning systems;
- Data input/output control, including portable devices;
- Application control and user management

And must include, at a minimum, the following:

1) A weekly full system scan for viruses and malware;
2) Signatures updated and maintained at current vendor supported and recommended levels;

All users are prohibited from disabling, circumventing or altering implemented security safeguards on state agency systems (e.g. firewalls, malicious code protection mechanisms) without prior written approval. (See 12.1.2)

In addition, all users are prohibited from downloading, installing, or otherwise using unauthorized software on state agency computers without first following established agency software asset inventory procedures. (See 12.5.1) Any software that would result in copyright violations must not be downloaded onto state systems.[47] All installed software applications within the agency must be inventoried and patched according to the Statewide Patch Management Standard.[48] All software must undergo security assessments and acceptance testing before being placed into production.

When technically possible the Agency will enable application whitelisting in all operating systems to ensure only authorized applications may be run on systems.

12.3 Backups

Objective: To protect against loss of data.

12.3.1 Information backup

Backup copies of information, software, and system images will be taken and tested regularly in accordance with the Statewide Data Backup Standards.[49] This standard defines the organization's requirements for backup of information, software, and systems, as well as retention and protection requirements.

12.4 Logging and monitoring

Objective: To record events and generate evidence.

Information systems must be monitored and information security events recorded to detect unauthorized access to information and information systems. The agency must employ monitoring techniques to comply with applicable statewide policies related to acceptable use for state agency managed networks and systems.[50] An event is any observable occurrence in an information system. The Oregon Enterprise Security

[47] Statewide Acceptable Use of State Information Assets, para III
[48] Statewide Information Security Standards, para 5.9
[49] Statewide Information Security Standards, para 5.5
[50] Statewide Information Security Plan, 2009

Office identifies security events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate.[51]

12.4.1 Event logging

Statewide Log Management Standards provide guidance on log management and log review to proactively find security related events. For the complete log management standard details/requirements, see the Statewide Log Management Standard.[52] To detect unauthorized access to agency information and information systems, systems will be actively monitored and information security events recorded and reported. The agency will employ various monitoring techniques to comply with applicable statewide requirements.

12.4.2 Protection of log information

Log data must, by default, be considered at least Level 3, until sensitive Level 3 or Level 4 information has been removed (e.g. redacted) for public disclosure. If logs contain personally identifiable information, as defined in ORS 646A-600, federal or industry regulations (PCI), they must be protected in accordance with the most restrictive applicable regulations and laws.

12.4.3 Administrator and operator logs

The State of Oregon has developed standards that require protecting audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (e.g. audit records, audit settings, and audit reports) needed to successfully audit information system activity. System administrator and system operator activities will be logged and the logs protected and regularly reviewed. Where possible an intrusion detection system is used to monitor system and network administration activities for compliance. All devices, systems, and software must log the activities of privileged users. Logs recording privileged user activities must be descriptive, specific and granular. Additionally, privileged user activity must be logged, monitored, and specific behaviors alerted when a privileged user attempts to increase their privileges, when a privileged user attempts to modify logs, and when a privileged user attempts to create another account and assign privileges. (See 9.2.3)

12.4.4 Clock synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.[53] Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.[54] Agency system clocks must be synchronized with at least three separate authoritative time sources – with one source obtained from the State Data Center time service (ntp.state.or.us), or NIST Time Servers.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

[51] NIST SP 800-53r4, AU-2
[52] Statewide Information Security Standards, para 5.3
[53] ISO 27002:2013, 12.4.4
[54] NIST SP 800-53r4, AU-8

The use of all software is subject to a license agreement. This license agreement may have several names (EULA, ELA, EA, CLP, etc.); it may even appear as a click-through on a web site. At a high level, a license agreement sets forth the terms and conditions related to the use of the software program; it's the list of what the end user (or the agency) can or cannot do with the software, and often sets forth the consequences for violating the agreement. Any software that would result in copyright violations must not be downloaded onto state systems. The agency leadership is responsible for ensuring it has a license agreement that meets the state's requirements for all software that is in use by its employees, contractors or agents. Additionally, agency management with procurement abilities must be familiar with ORS 291.047, "Public contract approval by Attorney General", ORS 279A.140, "State procurement of goods and services, and OAR chapter 137, division 045, "Review of pubic contracts" prior to entering into information technology related contracts.

Where questions arise around software license agreements (e.g. legal sufficiency, establishing acceptable license agreements with software value added resellers, if the agreement is planned for statewide use, or if the software license is not otherwise exempt), the agency will contact DAS Procurement Services or the DOJ Business Transactions Section for further guidance.

The agency must have written software asset inventory procedures, which detail the processes (including acquisition), responsibilities, and technology for tracking and managing approved and unapproved software assets. The agency should use the latest version of the Center for Internet Security (CIS) controls framework for inventory and control guidance. (See 8.1.1)

All users are prohibited from downloading or installing software on state agency computers without first following established agency software asset inventory procedures. (See 12.2.1, 12.6.2)

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer system. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.[55]

Vulnerability Management

The ESO has established a statewide vulnerability management program to work in collaboration with the agency to monitor and report on IT systems, networks, and applications for security vulnerabilities (see definition).

The agency will assess security vulnerabilities reported by the ESO, classify them by severity level, communicate them to the System Owner, and prioritize them in terms of risk.

Where vulnerabilities are identified, but cannot be remediated within the required timeframe, the System Owner will evaluate the risks relating to the known vulnerability and define compensating controls – which may include appropriate detective and corrective actions. The agency must document the compensating controls that have been applied to adequately protect the information. The deviation document must be signed by the agency director, retained, and submitted to the OSCIO.

[55] NIST Special Publication 800-40 v2 (Superseded; definition used only for reference)

The agency must have written vulnerability management procedures, which detail the processes, responsibilities, and technology for the remediation of vulnerabilities. The agency should use the latest version of the Center for Internet Security (CIS) controls framework for continuous vulnerability management guidance.

Patch Management

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Patches serve other purposes than just fixing software flaws; they can also add new features to software and firmware, including security capabilities.

The agency must develop procedures to rapidly test and deploy critical patches to its systems in the event of a "patch now" advisory. For all other patching, the agency must deploy security patches to operating systems and applications within 30 days of release, unless the agency follows a documented procedure for testing and deploying security patches within an identified timeframe.[56]

The agency should use the latest version of NIST Special Publication 800-40, Guide to Enterprise Patch Management Technologies, for guidance in understanding the basics of patch management technologies, importance of patch management, and challenges in performing patch management.

12.6.2 Restrictions on software installation

All users are prohibited from downloading or installing software on state agency computers without first following established agency software asset inventory procedures. All installed software within the agency will be inventoried. Procedures must be developed to accommodate software purchases and installs and include software security assessments to identify and document baseline security configurations. All software approved for use by the Agency must abide by the End User License Agreement (EULA). (See 12.5.1)

If the agency chooses to allow users to use personal third-party computing systems or services (e.g. "cloud" providers, including but not limited to Microsoft OneDrive, Google Drive, and Dropbox), the agency must have a written procedure by which users are granted approval. All users must be granted approval, in accordance with the agency written procedure and in writing, prior to using of any third-party computing systems.

12.7 Information systems audit considerations

Objective: To minimize the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

In accordance with ORS 276A.306(3), the Agency must periodically conduct or contract for an information security assessment of the state agency's information system and information resources and shall request results from a third party's information security assessment of an information service that the third party provides and to which the state agency subscribes. Each state agency shall notify the Legislative Fiscal Office of the information security assessment after the state agency receives the results of the information security assessment.

Security assessments may be requested through the Secretary of State, the Enterprise Security Office, or third-party vendors. Security assessments may also include CJIS audits, Social Security Administration (SSA) audits, or other regulatory compliance audits.

[56] Statewide Information Security Standards, para 5.9.2

13 Communications Security

13.1 Network Security Management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

In locations where the agency manages its networks, the agency must establish security controls (e.g. firewalls, VLANs, ACLs) to safeguard the availability, confidentiality and integrity of information passing over its wired and wireless networks. (See also 9.2.1, 9.2.4, 9.4.3)

Appropriate logging and monitoring will be applied to enable recording and detection of actions that may affect, or are relevant to, information security. Compliance with Statewide Log Management Standards is compulsory.

13.1.2 Security of network services

Devices connected to a state agency network must comply with the Statewide Information Security Standards. Where devices cannot comply with the Statewide Information Security Standards, exceptions should be coordinated with the ESO and the State CISO. Devices that do not meet the minimum standards or that have not been approved for exception by the State CISO will be disconnected.[57] (See 9.1.2)

13.1.3 Network Segmentation

At a minimum, network segmentation will comply with the Statewide Local Area Network/Wide Area Network Statewide Information Security standards.[58] The agency will segment the network as required, creating not only a hardened perimeter, but also logical groupings of information systems divided into manageable network zones.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Procedures for handling and storing information must be established and communicated to protect information from unauthorized disclosure or misuse. Users must take appropriate precautions not to reveal confidential information. Exchange of Level 3 or higher information and software with other agencies and organizations is based on a formal exchange policy. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, media will be controlled and physically protected. Information must be protected against unauthorized access, misuse or corruption while at rest or during transportation, whether sent across networks or within state agency networks through the use of encryption.

13.2.2 Agreements on information transfer

Agreements to transfer information between other agencies or external parties must be established and maintained to protect information in transit based upon statewide information security standards. (See 8.3.3) Agreements may be electronic or manual, and may take the form of formal contracts.[59]

[57] Statewide Information Security Standard, para 6.1
[58] Statewide Information Security Standard, para 6.1.5
[59] ISO 27002:2013 13.2.2

13.2.3 Electronic messaging (e.g. Email, Instant messaging)

The Statewide Standards set the transmission requirement for all state agency information. The agency must follow the Statewide Standards for encryption of data in transit.[60] Level-3 and Level-4 information must be encrypted, whether sent across networks or within state agency networks and network segments.

Mobile device users should remain alert of their surroundings for suspicious activities (e.g. shoulder surfing, "free" Wi-Fi) when using mobile devices in public places, meeting rooms and other unprotected areas (see 6.2.1).

The use of electronic messaging must comply with the Statewide Acceptable Use of Information Assets policy.

13.2.4 Confidentiality or non-disclosure agreements

Agency confidentiality and non-disclosure agreements are reviewed periodically and when changes occur that influence these requirements.

[60] Statewide Information Security Standard, para 1.1 & 1.2

14 Information Systems Acquisition, Development and Maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes requirements for information systems which provide services over public networks.

Security requirements must be defined for ensuring that appropriate controls are programmed according to business needs. Management, working in conjunction with the system owner and the information owner, have the responsibility to ensure information security controls meet business requirements and provide secondary oversight.

14.1.1 Information security requirements within system security plans

The effective integration of security requirements into statewide and agency architecture also helps to ensure that important security considerations are directly related to the state agency mission/business processes. Therefore, the identification and management of information security requirements and associated processes must be integrated into early stages of information system projects.[61]

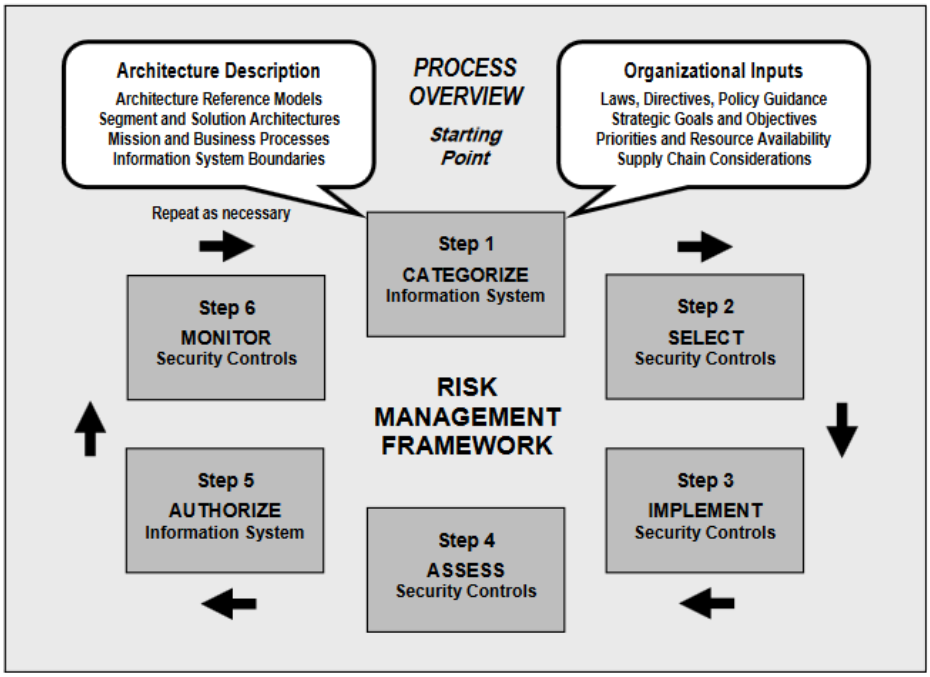

Figure 1: NIST Risk Management Framework as applied to the System Development Lifecycle process

By employing the Risk Management Framework (RMF) during the system development lifecycle process (see Figure 1), the agency emphasizes:

[61] ISO 27002:2013 14.1.1

(i) Building information security capabilities into its information systems through the application of organizational, operational, and technical security controls;
(ii) Maintaining awareness of the security of information systems on an ongoing basis through monitoring processes; and
(iii) Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, and other organizations arising from the operation and use of its information systems.

System security plans (SSPs), which are the product of the RMF applied to the information system during the system development/acquisition lifecycle process, should be started at project initiation and define, at a minimum; system function or purpose, system boundaries, contact information, classification of the system (see Appendix B, Table 1), information classification types that will be stored on or processed by the system (See 8.2.1),and any interconnections with other systems (e.g. identifying systems that transmit or receive information with the system). In later phases of the system development lifecycle, SSPs describe, at a detailed technical level, how the security controls and control enhancements meet those security requirements. Before the system is permitted to be placed into production, the authorizing official is provided with the SSP, security assessment, and the plan of action and milestones to make a risk-based authorization decision. (See 14.2.9)

The agency should reference the latest revision of NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, to assist in conducting the activities of SSP development and NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, to assist in the selection and understanding of security controls.

Systems requiring an SSP include, but are not limited to; 1) Systems accessible from the internet, 2) Systems that process, store, or generate Level 3 or higher information, 3) Systems categorized with a potential business impact to the agency as 'moderate' or 'high' (See Appendix B, Table 1 & 14.2.9), and 4) systems that require oversight. Additionally, where systems require oversight, SSPs will be submitted to the OSCIO for approval.

All SSPs must be reviewed annually.[62]

The Enterprise Security Office will assist as an advisor, at the request of the agency, in the development of SSPs.

Security training can help ensure individuals who have key roles and responsibilities have the knowledge, skills, and expertise to conduct assigned system development life cycle activities.

14.1.2 Securing application services on public networks

Boundary protection must be in place for monitoring and controlling communications to application services accessible from public networks through its security architecture. Protection technologies include firewalls, intrusion detection systems, and network segmentation that physically separates publicly accessible systems from internal agency networks. Additionally, the agency must comply with the Statewide Cryptography and Communications Security Standard to protect the confidentiality of information and help prevent unauthorized disclosure.

14.1.3 Protecting application services transactions

Information involved in application service transactions will be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, or unauthorized disclosure. Information security considerations include all aspects of the transaction (e.g. ensuring that the user's secret authentication information is valid and verified, that the transaction remains confidential, that privacy is retained), communications are encrypted,

[62] NIST Special Publication 800-53, PL-2

protocols are secured, and ensuring that the storage of information is commensurate with information classification level and handling standards.[63]

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

The Statewide Standard - Information System Development Lifecycle Recommended Best Practices, provides the identification of security concerns before actual coding begins, that security requirements be incorporated into the design of applications, and that secure coding practices are observed. All project managers, developers, and testers should be familiar with statewide information security policies and standards and formally trained in secure coding practices. To enhance and improve secure application development, information security resources, such as the Open Web Application Security Project (OWASP) and NIST Special Publication 800-64, must be made freely available and encouraged early in the project lifecycle.

Compliance is assessed through application security testing, which includes testing for secure coding principles described in the OWASP Secure Coding Guidelines (See Appendix C).

While OWASP specifically references web applications, the secure coding principles outlined above should be applied to non-web applications as well.

The agency should also reference the latest revision of NIST Special Publication 800-64, Security Considerations in the System Development Lifecycle, to assist in building security into the software development processes.

14.2.2 System change control procedures

Changes to systems within the development lifecycle will be controlled by the use of formal change control procedures. Introduction of new systems and major changes to existing systems will follow a formal process of documentation, specification, testing, quality control, and managed implementation. This process should include a risk assessment, quality assurance, analysis of the impacts of changes and specification of security controls needed. It should also ensure that existing security and control procedures are not compromised.

14.2.3 Technical review of applications after operating platform changes

Personnel with information security expertise are required as part of the change control process. Representation by information security personnel is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of agency systems.[64]

14.2.4 Restrictions on changes to software packages

Modifications to software packages is discouraged. All changes will be strictly controlled and limited only to what is necessary and allowed by contract. As far as possible and practicable, vendor-supplied software packages will be used without modification. Where a software package needs to be modified, the following should be considered:

1) The risks of built-in controls and integrity processes being compromised,
2) Whether the consent of the vendor should be obtained,
3) The possibility of obtaining the required changes from the vendor as standard program updates,

[63] ISO 27002:2013 14.1.3
[64] NIST SP 800-53r4, CM-3, CM-4

4) The impact if a state agency becomes responsible for the future maintenance of the software as a result of changes, and
5) Compatibility with other software in use.

All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades.[65]

14.2.5 Secure system engineering principles

The agency will apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Security engineering principles include, for example: developing layered protections, establishing sound security policy, architecture, and controls as the foundation for design, delineating physical and logical security boundaries, ensuring that the system developers are trained on how to build secure software, tailoring security controls to meet organizational and operational needs, and reducing risk to acceptable levels, thus enabling informed risk management decisions.[66]

14.2.6 Secure development environment

A secure development environment includes people, processes and technology associated with system development and integration. The agency must establish and appropriately protect secure environments for system development and integration by assessing risks. In addition, the agency must establish secure environments considering sensitivity of information, trustworthiness of personnel (see 7.1.1), the need for network separation (see 12.1.4), control of access, monitoring of changes, the storage of code, backups, and control over movement of information.

14.2.7 Outsourced development

The agency must ensure third-party partners that are providing development services comply with all applicable laws, policies, plans, procedures, and standards.[67] Additionally, the agency must supervise, log, and audit all activities of third-party partners while connected to agency systems.

14.2.8 System Security testing

Developmental security testing/evaluation must occur at all design phases of the system development life cycle, as well as major updates or fixes (see 14.2.2). Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements.[68] Prior to placing systems into production, systems must be scanned for vulnerabilities and CIS basic compliance.

14.2.9 System acceptance testing

System Security Plans (SSPs) ensure that information security is built into organizational information systems, and help to identify weaknesses and deficiencies early in the development process. SSPs also provide essential information needed to make risk-based decisions as part of security authorization processes, and ensure compliance to vulnerability mitigation procedures. The agency will develop SSPs for each system including, but not limited to; 1) Systems accessible from the internet, 2) Systems that process, store, or generate Level 3 or higher information, 3) Systems categorized with a potential impact by the system owner as ‘moderate’ or

[65] ISO 27002:2013, 14.2.4
[66] NIST SP 800-53r4, SA-8
[67] Cloud Computing Policy, para I
[68] NIST SP 800-53r4, SA-11

'high'(see Appendix B, Table 1), and 4) Systems that require oversight. SSPs will describe the scope of the system, including security controls and control enhancements, and roles and responsibilities (See 14.1.1).

As part of the system acceptance process, the agency will obtain a security baseline scan that includes, but is not limited to, software inventory, host-based firewall configuration, software vulnerabilities, and compliance audits for the system and added services, where applicable. SSP assessments for system acceptance testing should also include, for example, static analysis, dynamic analysis, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine. [69] These reports should be saved with the SSP for future reference.

Before the system is permitted to be placed into production, the authorizing official (see 6.1.1.1) is provided with the SSP (containing the identified system risks) and a plan of action and milestones to make a risk-based authorization decision. Additionally, where systems require oversight, SSPs will be submitted to the OSCIO for approval.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

The use of production data containing Level 3 or higher data, personally identifiable information (PII) or any other confidential information, for testing or developmental purposes is not allowed. Any deviation allowing Level 3 or higher, PII or otherwise confidential information to be used for testing purposes must document the business reason, compensating controls, and be approved in writing by the Agency Head. The approval must be retained by the agency. All sensitive details and content must be protected by removal or modification. (See 12.1.4)

When removal or modification is unavoidable, the following must be applied:

a) The access control procedures, which apply to production application systems, must also apply to test and dev application systems;
b) There must be separate authorization each time production information is copied to a test or dev environment;
c) Operational information must be erased from a test or development environment immediately after the testing is complete;
d) The copying and use of production information should be logged to provide an audit trail.

[69] NIST SP 800-53r4, SA4, SA12(7)

15 Third-party Relations

15.1 Information security in third-party relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

The agency must identify and mandate information security controls to specifically address third-party services to agency information. These controls address processes and procedures that are implemented by the agency, as well as process and procedures that the agency requires third-party partners to implement.[70] All third-party partners with whom the agency exchanges information must give evidence of requirements and capabilities to protect state information in compliance with, at a minimum, statewide information security policies.[71]

15.1.1 Information security policy for third-party relationships

Users who engage, contract with, or exchange information with third parties for cloud services, whether they be other state agencies, or external for-profit corporations, must adhere to the Statewide Cloud Computing Policy governing third-party partners. The agency will assess the security of all third parties with whom the agency exchanges information.

15.1.2 Addressing security within third-party agreements

The agency must comply with the Statewide Cloud Computing policy that establishes standards to ensure that benefits, costs, and risks to the state are appropriately analyzed and documented before contracting with third-party partners. In addition, it ensures that the readiness of the third-party partner is assessed to deliver a solution that meets the state's requirements. Security planning is conducted to ensure that state information and financial assets are appropriately protected. All agreements must include terms and conditions required by the Attorney General in order for the agreement to be approved for legal sufficiency in accordance with ORS 291.047. Agreements must use available forms and templates developed by DAS and the Department of Justice in accordance with ORS 279A, including the completed contractor's insurance requirement exhibit.[72]

15.1.3 Information and communication technology supply chain

The following should be considered for inclusion in agreements:

- Obtaining assurance that critical components, e.g. software, and their origin can be traced throughout the supply chain,
- The delivered information and communication technology products are functioning as expected without any unexpected or unwanted features,
- Acceptable methods for validating that information and communication technology products and services adhere to agency and statewide security requirements.

15.2 Third-party service delivery management

Objective: To maintain an agreed upon level of information security and service delivery.

15.2.1 Monitoring and review of third-party services

Monitoring and review of supplier services ensures that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

[70] ISO 27002:2013 15.1.1
[71] Statewide Cloud Policy, General Information, Requirements, paragraph I
[72] Statewide Cloud Computing policy

If third-party partners transmit or otherwise make state agency information available to an additional party (including making use of software as a service, infrastructure as a service, or the "cloud") the agency will require the third-party partner to assure the security of the additional party in a manner consistent with the agency and statewide information security requirements. The third-party partner must also provide evidence of such assurance and validation to the agency.

The agency should work with the DOJ to include "right to audit" clauses with third-party partners during contract negotiation and renewals.

15.2.2 Managing changes to third-party services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

The following aspects should be taken into consideration:

a) Changes to supplier agreements;
b) Changes made by the organization to implement:
    a. Enhancements to the current services offered;
    b. Development of any new applications and systems;
    c. Modifications or updates of the organization's policies and procedures;
    d. New or changed controls to resolve information security incidents and to improve security;.
c) Changes in supplier services to implement:
    a. Changes and enhancement to networks;
    b. Use of new technologies;
    c. Adoption of new products or newer versions/releases;
    d. New development tools and environments;
    e. Changes to physical location of service facilities;
    f. Change of suppliers;
    g. Sub-contracting to another supplier.

16 Information Security Incident Management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

The agency must comply with the Statewide Information Security Incident Response Policy and Plan that requires the agency to develop an incident response plan; processes and procedures to implement the plan; notify of reportable incidents to the ESO Security Incident Response Team (SIRT); and designate of an agency point of contact for the State Incident Response Team. Additionally, the agency incident response plan must be developed and align with the Statewide Information Security Incident Response plan.

16.1.1 Responsibilities and procedures

Responsibilities and procedures are established in the Statewide Information Security Incident Response Policy and Statewide Information Security Incident Response Plan to handle information security incidents and vulnerabilities once they have been reported. The agency must align the agency incident response responsibilities and procedures with the Statewide Information Security Incident Response Plan.

16.1.2 Reporting information security Incidents

The Statewide Information Security Incident Response Plan provides incident notification procedures. All users must be provided awareness training and are made aware of their responsibility to report information security events as quickly as possible. These responsibilities include reporting lost or stolen information assets (e.g. documents containing PII, laptop, USB drive, mobile phone), unauthorized access to information, conversation containing sensitive information overheard, and any kind of sabotage that effects information. When appropriate, the agency's management meetings should include discussion of information security issues. Agency newsletters can serve as a forum for discussing incident response issues.

The agency must report information security incidents to ESO no later than 24 hours after discovery.[73]

16.1.3 Reporting information security weaknesses

Information security incidents and weaknesses associated with information systems will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users.

16.1.4 Assessment of and decision on information security events

The agency must follow the Statewide Incident Response Plan for the assessment of and decision on information security events. The agency incident response team will classify incidents reported according to the criteria established in the plan. The agency incident response team may reclassify and escalate incidents as conditions change.

16.1.5 Response to information security incidents

Information security incidents must be responded to in accordance with the Statewide Information Security Incident Response Plan. These responses include evidence collection, forensics analysis, and escalation, ensuring all response activities are properly logged, communicating the existence of the information security incident to other internal and external entities, and formally closing and recording it. Post-incident analysis should take place, as necessary, to identify the source of the incident.

[73] Statewide Information Security Incident Response policy, Reporting Information Security Incidents

16.1.6 Learning from information security incidents

The agency must incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and must implement the resulting changes accordingly. The Statewide Information Security Incident Response Plan provides guidance on creating a follow-up report to correlate lessons learned in a post-incident activity.

16.1.7 Collection of evidence

The agency must define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. If needed or requested, the ESO Security Incident Response Team (SIRT) may perform various roles in responding to the incident, including evidence collection and forensic analysis.

17 Business Continuity Management and Continuity of Operations

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process is established to minimize the impact on agency business and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls. A managed process is developed and maintained for business continuity throughout the agency that addresses the information security requirements needed for agency business continuity.

DAS Statewide policy, 107-001-010, requires all State of Oregon agencies, individually, and in conjunction with other agencies, to develop, implement, test, maintain and execute Continuity of Operations Plans (COOP).[74] The policy establishes the basic principles and framework necessary to ensure emergency response, resumption, restoration, and permanent recovery of agency operations and business activities during a business interruption event.

The COOP improves an agency's resilience by identifying, in advance, the potential impacts of a wide variety of sudden disruptions to the agency, and by developing mitigation and contingency strategies that will improve the agency's ability to resume critical business functions in a relatively short time-frame.

The agency must develop, implement, and maintain the COOP, including identifying recovery alternatives.[75] The agency head is responsible for overall plan development. The agency head must designate someone to serve as the COOP sponsor, and a staff person to serve as the COOP coordinator. The COOP sponsor and coordinator will take responsibility for managing the COOP planning process.[76]

To ensure that the agency maintains a current and functional business continuity plan, the agency must update the plan annually, at a minimum.

[74] Statewide Continuity of Operations Planning, Purpose
[75] Statewide Continuity of Operations Planning, Policy Guidelines (III)
[76] Statewide Continuity of Operations Planning, Policy Guidelines (I & II)

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: state statute, regulations, statewide and agency policy, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information. Regulations governing compliance include but are not limited to:

- ORS 276A.300
- Oregon Consumer Identity Theft Protection Act (ORS 646A.600 to 646A.628)
- Statewide security policies
- Statewide Information Security Standards

Controls are established to maximize the effectiveness of the information systems audit process. During the audit process, controls safeguard operational systems and tools to protect the integrity of the information and prevent misuse.

The agency will comply with OAR 125-700-0020, which requires an internal audit function. The Internal Audit Section will consider information security when conducting risk assessments and developing the yearly audit plan.

As required by ORS 276A.300, the agency must send information security audits and assessment findings to the OSCIO.

18.1.2 Intellectual property rights

The agency uses software and associated documentation in accordance with contract agreements and copyright laws. Software will only be acquired through known and reputable sources, to ensure that copyright is not violated. Installation of software will be recorded and tracked for licensing purposes with regular reviews that ensure only authorized software and licensed products are installed. (See 12.5.1) All users are prohibited from downloading, installing, or otherwise using unauthorized software on state agency computers. (See 12.6.2)

18.1.3 Protection of records

Records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, Statewide Information Security standard, and the Statewide Information Asset Classification Policy. In addition, all users will comply with the asset management section and access control section of this plan and their related references.

18.1.4 Privacy and protection of personally identifiable information (PII)

The Privacy Act of 1974 and the Oregon Consumer Identity Theft Protection Act, ORS 646A.600 to 646A.628, define personal information. Through implementation of training and awareness strategy, the agency must promote a culture of privacy. The agency will develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and agency procedures for handling PII. Basic privacy training (e.g. the protection of PII) should be provided to all users that handle,

process, or store PII. Online training is available by contacting the Training and Awareness Coordinator at the ESO. (See also 8.2, 11.2.9)

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organization policies and procedures.

18.2.1 Independent review of information security

Each biennium, the ESO will be responsible for ensuring that an assessment of the agency's information systems program be conducted.[77] Agencies are required to cooperate with these assessments. All areas covered within this information security plan may be assessed, including a review of compliance with statewide and agency information security rules, policies, and standards.[78] Assessment results will specifically be provided to the agency, the State CISO, the Legislative Fiscal Office and the State CIO.[79]

18.2.2 Compliance with security plan, policies, standards, and procedures

At a minimum, compliance to this information security plan, and all published statewide policies and standards is mandatory. Pursuant to the ORS 276A.300 and the Statewide Information Security policy, each state agency head is responsible for ensuring his/her agency's compliance with state enterprise security policies, standards, and security initiatives, and with state and federal security regulations. Where the agency has published its own policies and standards in place of the statewide policy and standard, the most restrictive will be enforced. (See 7.2.2)

In circumstances where this plan, or portions of this plan, can/will not be implemented, the agency must document the deviations in an agency memorandum. The memorandum will list the deviations in a bulleted format, referencing the paragraph number, reason for the deviation, expected duration, and indicate what compensating controls have been applied to adequately protect information. The agency memorandum must be signed by the agency head, retained and submitted to the ESO.

Where the agency needs to append portions of this security plan (e.g. to prescribe agency policies, standards, and procedures that exceed statewide information policies and standards), those portions may be documented in the Agency Addendums section of this plan. (See Agency Addendums)

Where there is a conflict between this plan and statewide policies and standards, statewide policies and standards will supersede this information security plan.

18.2.3 Technical compliance review

Information systems will be regularly reviewed for compliance with the statewide information security policies and standards, as well as any local agency information security policies and standards. Technical compliance will be reviewed with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer may be performed.

The agency may request assistance from the ESO to perform their own technical compliance reviews of systems. Additionally, during periodic assessments or systems acquisition, development and maintenance, compliance reviews may be conducted. Special consideration may be made for systems accessible from the internet, systems

[77] ORS 276A.300(3)(c)
[78] ORS 291.039(4)(G)
[79] ORS 276A.300(8)(b)

that process, store, or generate Level 3 or higher information, or systems categorized with a potential impact by the system owner as ‘moderate’ or ‘high’ (See Appendix B, Table 1 , 14.1, 14.2.9)

19 Implementation

ORS 276A.300 requires the agency to secure computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information outside the state’s shared computing and network infrastructure, and follow information security standards, policies and procedures established by the State Chief Information Officer.

Where required, this plan gives direction and support for the agency to further define local information security policies, standards and procedures that may be developed in conjunction with this plan.

This information security plan, statewide policies and standards are living documents. The very nature of information assets and systems are subject to constant change. Changes can come from all levels – federal and state laws, the governing board, executive management, business or policy changes, and front line employees. Whenever changes in the threat environment occur, the Enterprise Security Office will update relevant documentation. This plan, as well as related policies and standards, will become an integral part of everyday agency operations.

In order to implement and properly maintain a robust information security function, the agency recognizes the importance of:

- Understanding information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage information security risks in the context of overall business risks;
- Ensuring all users of agency information assets are aware of their responsibilities in protecting those assets;
- Monitoring and reviewing the performance and effectiveness of information security policies and controls; and
- Continual improvement based on assessment, measurement, and changes that affect risk.

By instituting this information security plan, the agency intends to meet the following information security goals:

- Support and comply with statewide policies, best practices, and information security efforts;
- Have strong security policies, procedures, and processes in place to ensure information security objectives of availability, confidentiality, and integrity are met;
- Ensure employees are well-versed in information security policies and understand their role in information security;
- Effectively work with partners (DAS, vendors, etc.) to ensure information security objectives are being met;
- Proactively identify and mitigate risks to information as they emerge; and,
- Ensure the agency reacts in a timely manner to investigate and take appropriate action on potential security breaches.

APPROVAL

/Signed copy on file at ESO/ August 2018
Terrence Woods Date
State Chief Information Officer

/Signed copy on file at ESO/ August 2018
Stefan Richards Date
State Chief Information Security Officer

Appendix A – Controls Mapping

Table A-1 provides a mapping from the security controls in the Center for Internet Security (CIS) Critical Security Controls (CSC) to the security controls in NIST SP800-53 and the Statewide Security Plan. CSC is being used to prioritize efforts in implementation of the Statewide Security Plan. NIST SP800-53 provides detailed control guidance and explanations.

Table A - 1 : CSC Controls to NIST 800-53 to Statewide Plan

Critical Security Control	NIST 800-53 rev4	Statewide Plan
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	CA-7: Continuous Monitoring CM-8: Information System Component Inventory IA-3: Device Identification and Authentication SA-4: Acquisition Process SC-17: Public Key Infrastructure Certificates SI-4: Information System Monitoring PM-5: Information System Inventory	8.1.1 9.1.2 13.1.1
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-8: Information System Component Inventory CM-10: Software Usage Restrictions CM-11: User-Installed Software SA-4: Acquisition Process SC-18: Mobile Code SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring PM-5: Information System Inventory	12.5.1 12.6.2
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	CA-2: Security Assessments CA-7: Continuous Monitoring RA-5: Vulnerability Scanning SC-34: Non-Modifiable Executable Programs SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity	12.6.1 14.2.8
Critical Security Control #4: Controlled Use of Administrative Privileges	AC-2: Account Management AC-6: Least Privilege AC-17: Remote Access AC-19: Access Control for Mobile Devices CA-7: Continuous Monitoring IA-2: Identification and Authentication (Organizational Users) IA-4: Identifier Management IA-5: Authenticator Management SI-4: Information System Monitoring	9.1.1 9.2.2 - 9.2.6 9.3.1 9.4.1 - A.9.4.4
Critical Security Control #5: Secure Configurations for Hardware and Software	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices	14.2.2 14.2.4 14.2.8 18.2.3

	SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring	
Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs	AC-23: Data Mining Protection AU-2: Audit Events AU-3: Content of Audit Records AU-4: Audit Storage Capacity AU-5: Response to Audit Processing Failures AU-6: Audit Review, Analysis, and Reporting AU-7: Audit Reduction and Report Generation AU-8: Time Stamps AU-9: Protection of Audit Information AU-10: Non-repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-13: Monitoring for Information Disclosure AU-14: Session Audit CA-7: Continuous Monitoring IA-10: Adaptive Identification and Authentication SI-4: Information System Monitoring	12.4.1 - 12.4.4 12.7.1
Critical Security Control #7: Email and Web Browser Protections	CA-7: Continuous Monitoring CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-7: Least Functionality CM-8: Information System Component Inventory CM-9: Configuration Management Plan CM-11: User-Installed Software MA-4: Nonlocal Maintenance RA-5: Vulnerability Scanning SA-4: Acquisition Process SC-15: Collaborative Computing Devices SC-34: Non-Modifiable Executable Programs SI-2: Flaw Remediation SI-4: Information System Monitoring	14.2.4 14.2.8 18.2.3
Critical Security Control #8: Malware Defenses	CA-7: Continuous Monitoring SC-39: Process Isolation SC-44: Detonation Chambers SI-3: Malicious Code Protection SI-4: Information System Monitoring SI-8: Spam Protection	8.3.1 12.2.1 13.2.3
Critical Security Control #9: Limitation and Control of Network Ports	AC-4: Information Flow Enforcement CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-6: Configuration Settings CM-8: Information System Component Inventory SC-20: Secure Name /Address Resolution Service (Authoritative Source) SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver) SC-22: Architecture and Provisioning for Name/Address Resolution Service SC-41: Port and I/O Device Access SI-4: Information System Monitoring	9.1.2 13.1.1 13.1.2 14.1.2

Critical Security Control #10: Data Recovery Capabilities	CP-9: Information System Backup CP-10: Information System Recovery and Reconstitution MP-4: Media Storage	10.1.1 12.3.1
Critical Security Control #11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	AC-4: Information Flow Enforcement CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration CM-3: Configuration Change Control CM-5: Access Restrictions for Change CM-6: Configuration Settings CM-8: Information System Component Inventory MA-4: Nonlocal Maintenance SC-24: Fail in Known State SI-4: Information System Monitoring	9.1.2 13.1.1 13.1.3
Critical Security Control #12: Boundary Defense	AC-4: Information Flow Enforcement AC-17: Remote Access AC-20: Use of External Information Systems CA-3: System Interconnections CA-7: Continuous Monitoring CA-9: Internal System Connections CM-2: Baseline Configuration SA-9: External Information System Services SC-7: Boundary Protection SC-8: Transmission Confidentiality and Integrity SI-4: Information System Monitoring	9.1.2 12.4.1 12.7.1 13.1.1 13.1.3 13.2.3
Critical Security Control #13: Data Protection	AC-3: Access Enforcement AC-4: Information Flow Enforcement AC-23: Data Mining Protection CA-7: Continuous Monitoring CA-9: Internal System Connections IR-9: Information Spillage Response MP-5: Media Transport SA-18: Tamper Resistance and Detection SC-8: Transmission Confidentiality and Integrity SC-28: Protection of Information at Rest SC-31: Covert Channel Analysis SC-41: Port and I/O Device Access SI-4: Information System Monitoring	8.3.1 10.1.1 - 10.1.2 13.2.3 18.1.5
Critical Security Control #14: Controlled Access Based on the Need to Know	AC-1: Access Control Policy and Procedures AC-2: Account Management AC-3: Access Enforcement AC-6: Least Privilege AC-24: Access Control Decisions CA-7: Continuous Monitoring MP-3: Media Marking RA-2: Security Categorization SC-16: Transmission of Security Attributes SI-4: Information System Monitoring	8.3.1 9.1.1 10.1.1
Critical Security Control #15: Wireless Access Control	AC-18: Wireless Access AC-19: Access Control for Mobile Devices CA-3: System Interconnections CA-7: Continuous Monitoring CM-2: Baseline Configuration IA-3: Device Identification and Authentication SC-8: Transmission Confidentiality and Integrity	10.1.1 12.4.1 12.7.1

	SC-17: Public Key Infrastructure Certificates SC-40: Wireless Link Protection SI-4: Information System Monitoring	
Critical Security Control #16: Account Monitoring and Control	AC-2: Account Management AC-3: Access Enforcement AC-7: Unsuccessful Logon Attempts AC-11: Session Lock AC-12: Session Termination CA-7: Continuous Monitoring IA-5: Authenticator Management IA-10: Adaptive Identification and Authentication SC-17: Public Key Infrastructure Certificates SC-23: Session Authenticity SI-4: Information System Monitoring	9.1.1 9.2.1 - 9.2.6 9.3.1 9.4.1 - 9.4.3 11.2.8
Critical Security Control #17: Implement a Security Awareness and Training Program	AT-1: Security Awareness and Training Policy and Procedures AT-2: Security Awareness Training AT-3: Role-Based Security Training AT-4: Security Training Records SA-11: Developer Security Testing and Evaluation SA-16: Developer-Provided Training PM-13: Information Security Workforce PM-14: Testing, Training, & Monitoring PM-16: Threat Awareness Program	7.2.2
Critical Security Control #18: Application Software Security	SA-13: Trustworthiness SA-15: Development Process, Standards, and Tools SA-16: Developer-Provided Training SA-17: Developer Security Architecture and Design SA-20: Customized Development of Critical Components SA-21: Developer Screening SC-39: Process Isolation SI-10: Information Input Validation SI-11: Error Handling SI-15: Information Output Filtering SI-16: Memory Protection	9.4.5 12.1.4 14.2.1 14.2.6 - A.14.2.8
Critical Security Control #19: Incident Response and Management	IR-1: Incident Response Policy and Procedures IR-2: Incident Response Training IR-3: Incident Response Testing IR-4: Incident Handling IR-5: Incident Monitoring IR-6: Incident Reporting IR-7: Incident Response Assistance IR-8: Incident Response Plan IR-10: Integrated Information Security Analysis Team	6.1.3 7.2.1 16.1.2 16.1.4 - 16.1.7
Critical Security Control #20: Penetration Tests and Red Team Exercises	CA-2: Security Assessments CA-5: Plan of Action and Milestones CA-6: Security Authorization CA-8: Penetration Testing RA-6: Technical Surveillance Countermeasures Survey SI-6: Security Function Verification PM-6: Information Security Measures of Performance PM-14: Testing, Training, & Monitoring	14.2.8 18.2.1 18.2.3

Appendix B – Categorization of Information and Information Systems

Categorization of State of Oregon Information and Information Systems

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Appendix C – OWASP Secure Coding Guidelines

Compliance is assessed through application security testing, which includes testing for secure coding principles described in the OWASP Secure Coding Guidelines:

- Input Validation
- Output Encoding
- Authentication and Password Management (includes secure handling of credentials by external services/scripts)
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

Index

Agency Addendums

The Agency adopts the Statewide Information Security Plan. This Addendum modifies and supplements the attached Statewide Information Security Plan with the following additions, deletions, modifications, or clarifications:

<Begin Example>

<State the paragraph number, heading, and in parenthesis identify as an addition, deletion, modification, or clarification, and a narrative of how the agency addresses the requirement. If necessary cite federal or other regulatory requirements.>

Para 6.2.1 Mobile Device Policy (Addition):

The management of mobile devices is the responsibility of the <organization name> organization and outside of the scope of the Agency. Mobile devices are not authorized for the use of management of agency systems, and only approved for email and calendaring and for internal Agency communications.

Agency policy does not allow the use of mobile devices for the support, management or access of regulated data.

Para 9.1.2 Access to networks and network services (Modification):

Devices connected to a state network must comply with established statewide policies and standards. Devices that do not meet the minimum statewide network security standard require an exception by the State CISO or will be disconnected. ***Non-state agency owned portable devices are prohibited from connecting to state networks.***

Para 12.6.1 Management of Technical Vulnerabilities

Patch Management (Clarification):

Agency servers are hosted at the State Data Center. All OS patching will be performed by State Data Center technicians, per their written procedures. The State Data Center and Agency technicians will coordinate patching activities based upon business requirements. All application patching will be performed by Agency technicians, per Agency written patch management procedures.

Para 14.2.1 Secure development policy (Clarification):

The Agency does not perform software development.

<End Example>