2023 Statewide Information Security Program Plan

Date: July 2023

Date	Author	Version	Change Reference
11/15/22	Paul LaVigne	1.0	Initial Version
7/20/23	Paul LaVigne	1.1	Collaborated Draft
12/8/23	Paul LaVigne, Adam Mele	1.2	Final Review

1 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 *National Institute of Standards and Technology's* (NIST) *SP800-53.*

2 Document Scope

The requirements documented herein are based on the *Statewide Standards*, which were developed to align with NIST SP800-53 and informed by the State Risk and Authorization Management Program (StateRAMP). 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.

3 Purpose and Applicability

The purpose of this Information Security Program Plan is to outline the activities that are required to constitute a cybersecurity program within the State of Oregon Enterprise. These activities include cybersecurity efforts and projects that:

- Require regular input, authorization, and review from leadership
- Span large periods of time, as opposed to a one-time configuration setting, or process.
- Require coordination across multiple sub-controls or disciplines
- Produce documentable results
- Are supported by Statewide policies, plans, procedures, or standards

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.

3.1 Applicability

This plan applies to all Oregon Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 276A.300, 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.

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 reviewed at a minimum every two years, or as changes occur in the foundational reference framework, and updated as necessary.

3.2 Alignment

The State of Oregon has adopted the NIST family of cybersecurity controls, as well as the programmatic activities outlined in NIST SP800-53, in conjunction with StateRAMP. These controls are intended to not only utilize a well-respected and effective industry standard framework, but also streamline the selection of partner organizations that would ideally align to these same frameworks.

3.3 Target Audience

This document provides guidance and must be made available to all users and third-parties who access state information assets or are authorized to use state information technology.

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

3.4 Authority

3.4.1 Statutory Authority

ORS 276A.300 (2)
"The State Chief Information Officer has responsibility for and authority over information systems security in the executive department, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures. The plan must align with and support the Enterprise Information Resources Management Strategy described in ORS 276A.203 (State Chief Information Officer)."

3.4.2 Leadership and Commitment

The State of Oregon executive management demonstrates 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.

3.5 Shared Responsibilities

Given the evolution of IT infrastructure within the State of Oregon over the years, many agencies had developed independent IT and cybersecurity programs. Since the consolidation of cybersecurity under ORS 276A.300, all Enterprise-wide cybersecurity activities will be undertaken under the direction of, or in cooperation with, Cyber Security Services (CSS), whereas other operational responsibilities will remain in the agencies (ORS 276A.300 (8)). CSS has a current set of centralized Enterprise offerings, and that list will continue to grow as the programs mature. In addition to current offerings, agencies will implement new services offered, as well as adhere to all the governance outlined in this and other enterprise-wide policies, plans, procedures, and standards.

4 Terms and Definitions

For a list of common terms and definitions, please refer to Glossary A in the latest version of NIST SP800-53 Rev 5

5 Governance

5.1 Oregon Statutes and Administrative Rules

ORS/OAR Number	Title
ORS 646A.600	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
ORS 164.377	Computer Crime
OAR 125-800	State Information Security

5.2 Statewide 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
107-004-052	Information Security Policy
107-004-053	Employee Security
107-004-110	Acceptable Use of State Information Assets
107-004-120	Information Security Incident Response
107-004-150	Cloud and Hosted Systems
107-011-170	Building Security Access Controls

5.3 Statewide Information Security Standards

Standard Number	Standard Title
v1.0 (2023)	Statewide Information Technology (IT) Control Standards

6 Organization and Management

6.1 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.
Cyber Security Services (CSS)	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, 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, directives, and with state, federal, and industry regulations (ex HIPAA, PCI, CJIS, FIPS, FERPA, etc.).
Information Security Board	The governing body made up of agency executives and senior management; responsible for providing strategic direction, ensuring Chief Compliance/Audit/ Risk Officer (if applicable) that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the agency's resources are used responsibly. 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.

Information Systems Auditor (if applicable)	Responsible for planning, executing, and leading security audits across the agency.
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.[1] Users are responsible for complying with the provisions of plans, policies, standards, and procedures.

6.2 Governance Management

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 EIS 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 to validate the feasibility of statewide information security initiatives and strategies and make informed, clearly defined and prioritized recommendations to CSS.

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

[1] Acceptable Use of State Information Assets, Definitions

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.

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.*

6.3 Cybersecurity Governance Review

Information security policies must be reviewed at planned intervals of 2-3 years 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.

7 (AC) Access Control

Access to information, information systems, and information processing facilities are controlled according to business needs and information security requirements. 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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

8 (AT) Awareness 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.

As part of the CSS 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.

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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

9 (AU) Audit and Accountability

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 standards related to acceptable use for state agency managed networks and systems.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

10 (CA) Assessment, Authorization, and Monitoring

Agencies must assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) assessments from other regulated data organizations; (iii) continuous monitoring; and (iv) system development life cycle activities.

Security assessments ensure that information security is built into organizational information systems, identify weaknesses and deficiencies early in the development process, provide essential information needed to make risk-based decisions as part of security authorization processes, and ensure compliance to vulnerability mitigation procedures.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

11 (CM) Configuration Management

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

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

12 (CP) Contingency Planning

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.

Per policy, all State of Oregon agencies, individually, and in conjunction with other agencies, are required to develop, implement, test, maintain and execute Continuity of Operations Plans (COOP). 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. 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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

13 (IA) Identification and Authentication

Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in Statewide Standards, and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

14 (IR) Incident Response

Information security incidents affect the state's enterprise information assets and its ability to provide services to citizens of Oregon. Incidents must be investigated and a response prepared to mitigate the state's risk. Because of inter-related data processing and public perception of the State as a single entity, information security incidents at individual agencies may impact other state agencies or the State as a whole. Incident response activities must be effective, coordinated, and protect the interests of individual agencies, the state as a whole, and of the citizens they serve.

Incident Response describes how resources are to be brought together to respond to an information security incident. The objectives of the incident response plan are to facilitate quick and efficient response to incidents, limiting their impact and protecting State information assets. The incident response plan defines roles and responsibilities, documents the steps necessary for effectively managing an information security incident, describes incident severity levels and how escalation occurs, pre-defines communications channels and prescribes necessary education to achieve these objectives.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

15 (MA) Maintenance

Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations consider supply chain-related risks associated with replacement components for systems.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

16 (MP) Media Protection

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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards

17 (PE) Physical and Environmental Protection

Physical and Environmental protections must be in place in order to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

18 (PL) Planning

Planning is an integral part of all cybersecurity programs, to ensure clarity and consistency with all programmatic activities, ensure business alignment, improve maturity, promote coordination with organizational entities, establish rules of behavior, develop security architecture, and manage control baselines.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

19 (PM) Program Management

Management of the cybersecurity program is essential, to promote constant improvement and iterative steps to ensure that the Cybersecurity program remains relevant and effective with regards to the ever changing landscape of cybersecurity.

19.1 Applicable Standards

While not currently reflected in the statewide standards, the following additional programmatic controls from NIST SP800-53 Rev5 will also be included:

19.1.1 PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

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

19.1.2 PM-3 INFORMATION SECURITY RESOURCES

a. Include the resources needed to implement the information security in capital planning and investment requests and document all exceptions to this requirement;
b. Prepare documentation required for addressing information security in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and
c. Make available for expenditure, the planned information security resources.

19.1.3 PM-4 PLAN OF ACTION AND MILESTONES PROCESS

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

1. Are developed and maintained;
2. Document the remedial information security and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the State; and
3. Are reported in accordance with established reporting requirements.

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

19.1.4 PM-5 INFORMATION SYSTEM INVENTORY

The organization develops and maintains an inventory of its information systems.

19.1.5 PM-6 MEASURES OF PERFORMANCE

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

19.1.6 PM-7 ENTERPRISE ARCHITECTURE

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

19.1.7 PM-8 CRITICAL INFRASTRUCTURE PLAN

Address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

19.1.8 PM-9 RISK MANAGEMENT STRATEGY

a. Develop a comprehensive strategy to manage security risk associated with the operation and use of organizational systems to operations and assets, individuals, other organizations, and the State;
b. Implement the risk management strategy consistently across the organization; and
c. Review and update the risk management strategy annually or as required, to address organizational changes.

19.1.9 PM-10 AUTHORIZATION PROCESS

a. Manage the security of state of organizational systems and the environments in which those systems operate through authorization processes;
b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Integrate the authorization processes into an organization-wide risk management program.

19.1.10 PM-11 MISSION AND BUSINESS PROCESS DEFINITION

a. Define organizational mission and business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State;
b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
c. Review and revise the mission and business processes annually

19.1.11 PM-12 INSIDER THREAT PROGRAM

Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

19.1.12 PM-13 SECURITY WORKFORCE

Establish a security workforce development and improvement program.

19.1.13 PM-14 TESTING, TRAINING, AND MONITORING

a. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems:
    1. Are developed and maintained; and
    2. Continue to be executed;
b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

19.1.14 PM-15 SECURITY GROUPS AND ASSOCIATIONS

Establish and institutionalize contact with selected groups and associations within the security communities:
a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies; and
c. To share current security information, including threats, vulnerabilities, and incidents.

19.1.15 PM-16 THREAT AWARENESS PROGRAM

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

19.1.16 PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

a. Establish policy and procedures to ensure that requirements for the protection of organizational data that is processed, stored, or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards; and
b. Review and update the policy and procedures annually.

19.1.17 PM-21 ACCOUNTING OF DISCLOSURES

a. Develop and maintain an accurate accounting of disclosures of personally identifiable information, including:

1. Date, nature, and purpose of each disclosure; and
2. Name and address, or other contact information of the individual or organization to which the disclosure was made;

b. Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and
c. Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

19.1.18 PM-28 RISK FRAMING

a. Identify and document:

1. Assumptions affecting risk assessments, risk responses, and risk monitoring;
2. Constraints affecting risk assessments, risk responses, and risk monitoring;
3. Priorities and trade-offs considered by the organization for managing risk; and
4. Organizational risk tolerance;

b. Distribute the results of risk framing activities to organization-defined personnel; and
c. Review and update risk framing considerations.

20 (PS) Personnel Security

The agency will provide expectations 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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

21 (RA) Risk Assessment

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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

22 (SA) System and Services Acquisition

System Acquisition, development, and adoption must be handled appropriately, to ensure that vulnerabilities and faults are not introduced into existing systems, in both internally developed solutions, as well through as third-party acquisitions.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

23 (SC) System and Communication Protection

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.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

24 (SI) System and Information Integrity

Defensive measures must be put in place to ensure the Integrity of the State's data and systems by remediating flaws, preventing malware and malicious code, monitoring systems and communications, and blocking spam.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

25 (SR) Supply Chain Risk Management

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risk management (SCRM) activities include

identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans.

To accomplish these ends we have adopted the IT Controls in the current Statewide Information Technology (IT) Control Standards.

26 Adoption

Compliance to this information security plan, and statewide policies and standards is mandatory. All Executive Branch agencies, as defined in section 3.1 of this document, will use this plan to manage their information security programs. Pursuant to 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, security directives, and state and federal security regulations.

This plan outlines the minimum set of programmatic activities that an agency is expected to perform. 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 will ensure compliance with the more stringent legal/regulatory requirements. In areas where controls are required to meet state or federal regulation, CSS is committed to working in collaboration with the agency to meet the associated standards through consultative partnership and CSS provided services. Agencies must adopt policies that support the implementation of each of the IT Controls Standards. The policies must include agency roles and responsibilities associated with the control families contained with the Standards. Agency policies must be reviewed and updated biennially. A policy template is provided in Appendix B.

In circumstances where this plan, or portions of this plan, can/will not be implemented, the agency must document the deviation in accordance with the Statewide Cyber and Information Security Policy (107-004-052).

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 Appendix A below.

Appendix A

If an agency needs to perform additional activities for the purposes of addressing any agency-specific cybersecurity needs, then these will be recorded in this appendix. These may originate from regulated data, statutory requirements, or other internal needs.

1 Agency Specific Need

1.1 Description and details

This area is intended as a placeholder and intentionally blank for future agency-specific needs.

2 Agency Specific Need

2.1 Description and details

This area is intended as a placeholder and intentionally blank for future agency-specific needs.

Appendix B - Policy Template and Language

Policies can take many forms while being defined by each agency and their specific needs. For policy format, template, and more, please see the DAS Policies and Procedures page at https://stateoforegon.sharepoint.com/sites/DAS/SitePages/Policies.aspx

Additionally, NIST has published a Cybersecurity Framework Policy Template Guide, which provides policy language examples for each area of the NIST Cyber Security Framework (CSF). While many areas contain similar language and can be combined if desired, the document provides a starting point for organizations. The link below will provide a direct download of the NIST CSF Policy Template Guide.

https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf