ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES STATEWIDE POLICY	**NUMBER** 107-004-052	**SUPERSEDES** 107-004-052 | July 30, 2007
	EFFECTIVE DATE November 16, 2020	**PAGE NUMBER** Pages 1 of 5
	DATE OF LAST REVIEW November 16, 2020	
Division **Enterprise Information Services (State CIO)**	**REFERENCE** ORS 276A.300, 276A.303, 276A.306, 276A.323, 276A.326, 276A.329, 276A.332, 276A.335 OAR 125-800	
Policy Owner Cyber Security Services		
SUBJECT Cyber and Information Security	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer (Signature on file with DAS Business Services)	

PURPOSE

This policy establishes a unified and coherent statewide cyber and information security program to manage risks to state agency operations, information and information systems, and supporting infrastructure and services, while aligning cyber and information security with agencies' missions, goals and business operations.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

EXHIBITS/INSTRUCTIONS

The Statewide Information Security Plan and the Statewide Information and Cyber Security Standards can be found on the Cyber Security Services' (CSS) website: https://www.oregon.gov/das/OSCIO/Pages/SecurityGuidance.aspx.

Enterprise cyber and information security policies can be found on the Department of Administrative Services' website: https://www.oregon.gov/das/Pages/policies.aspx#IT.

CSS Exception Request Form can be obtained by agencies by emailing eso.info@oregon.gov.

DEFINITIONS

Availability: The principle of ensuring timely and reliable access to and use of information.

Confidentiality: The principle of preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

Cyber Security: The process of protecting information by preventing, detecting and responding to attacks.

Incident: A single or series of unwanted or unexpected information security events that result in harm or pose a significant threat of harm to information assets, an agency or third party, and which require non-routine preventive or corrective action.

Integrity: The principle of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

Information System: Computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

SPECIAL EXCEPTIONS

State agencies seeking an exception to this policy or cyber and information security program requirements must submit an exception request for approval by the State Chief Information Security Officer (CISO), using the CSS Exception Request Form. The CSS will review all exception requests to assess impact on enterprise risk.

GENERAL INFORMATION

The people of and businesses operating within Oregon have entrusted state government with information that they expect will be protected and secured. Information is a strategic asset that should be managed and secured as a valuable state resource.

(1) General Roles and Responsibilities

Protecting information security requires coordinated action by Enterprise Information Services (EIS), state agencies and individual users, all of whom play key roles in protecting state information assets.

(a) Enterprise Information Services – Chief Information Security Officer:

Within the EIS, the State CISO manages the state's information security program and serves as head of the CSS. The State CISO has overall responsibility for the development, implementation and performance of the cyber and information security program, including:

- Developing and maintaining administrative rules, policies, Statewide Information Security Plan, Statewide Information and Cyber Security Standards and other documentation.
- Managing a risk-based information technology security assessment and remediation program, including establishing enterprise risk and vulnerability management programs, policies and procedures.
- Providing unified enterprise solutions, technology, services and guidance to manage enterprise-level risks and assist agencies with implementing their own security programs.

- Identifying enterprise security requirements to limit the risks to state information assets.
- Developing, managing, and executing the enterprise cyber and incident response program.
- Implementing an enterprise information security awareness and training program.
- Providing information to and coordinating information sharing among state agencies regarding cyber security risks, threats, vulnerabilities and security measures.
- Providing information security subject matter expertise to state agencies.
- Maintaining security metrics to track the performance of the program.

In coordination with state agencies, CSS will maintain enterprise documents to establish cyber and information security program requirements and guide state agencies in meeting these requirements. These enterprise documents are comprised of:

- **Statewide Information Security Plan**: Defines the relevant safeguards for Oregon state agencies and state information systems, networks and applications.
- **Policies**: Document high-level rules, establish roles and responsibilities and set management expectations for information security practices. Policies complement the requirements outlined in the Statewide Information Security Plan.
- **Standards**: Identify a set of minimum requirements agencies must meet or approaches agencies must use when implementing the Statewide Information and Cyber Security Standards and information security policies. Agencies may elect to exceed these minimum security standards to achieve their organizational security goals and requirements.
- **Best Practices and Guidance**: Non-mandatory information that agencies may use to enhance the security of their information systems.

CSS will review the Statewide Information Security Plan, policies, and standards annually and update these documents, at minimum, every two years.

In addition, the CISO will define annual program priorities and implementation goals and provide this information to state agencies to guide program budgeting, planning and execution.

The CISO may also issue binding operational guidance to agencies specifying actions that agencies must implement to safeguard state information and information systems from a known or reasonably suspected information security threat, vulnerability or risk.

(b) **Agencies, Boards and Commissions:**

While it is the responsibility of all agency leadership, managers and staff to implement the requirements of this policy, the agency head is ultimately accountable for cyber and information security in their agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. Each agency head is responsible for:

- Providing clear direction and visible support for the cyber and information security program.
- Accepting cyber and information security risk on behalf of the agency.
- Ensuring the agency's compliance with the Statewide Information Security Plan, state policies, standards and initiatives, and with applicable federal and state laws and regulations.

Each agency must maintain a cyber and information security program to secure the information assets under its control. The basic agency program requirements include:

- Identifying responsibilities for cyber and information security management.
- Maintaining an inventory of agency hardware and software assets and categorizing assets based on their value to the agency and the business processes they support.
- Assessing threats, vulnerabilities and risks to agency information assets.
- Identifying security requirements to effectively limit cyber and information security risks associated with the agency's business goals and objectives.
- Establishing processes for incident identification and reporting.
- Implementing security education, training and awareness for all users of agency information assets.
- Communicating information security policies throughout the agency to users in a form that is relevant, accessible and understandable.

Each agency must comply with the Statewide Information Security Plan, state policies and standards. Agencies may either adopt the Statewide Information Security Plan and state policies or create their own plans and policies that comply with these documents. Each agency may, based upon its individual business needs or legal and regulatory requirements, exceed the security requirements established by CSS, but must, at a minimum, achieve the security objectives defined in those documents and may not conflict with those requirements. Agencies are responsible for developing internal procedures and guidance to implement their information security programs. Agencies will review and revise their information security plans, policies, standards and procedures in accordance with the Statewide Information Security Plan and the Statewide Information and Cyber Security Standards, as needed, every two years, at a minimum.

Agency information technology and risk environments are constantly evolving. Agencies will implement policies and procedures to regularly monitor and assess their cyber and information security programs. Agencies shall:

- Ensure that new business needs and risks are reflected in their information security plans and policies.
- Develop plans, in consultation with the EIS and CSS, for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement or retirement.

(c) **Users:**

Agency, board and commission full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities, collectively referred to as "users," are individuals authorized to access, and have a need to use, state information assets as part of their assigned duties or in fulfillment of assigned roles or functions. All users are governed by and responsible for complying with information security plans, policies, standards, and guidance and are accountable for their actions when using state information assets. All users are responsible for:

- Being aware of and complying with state and agency plans, policies, procedures, and standards and their responsibilities for protecting the information assets of their agency and the state.
- Using information resources only for intended purposes as defined by the policies, laws and regulations of the state or agency.

- Completing annual enterprise security training and role-specific security training, as well as participating in enterprise and agency security awareness and training initiatives as directed.

(2) **Enterprise Security Baseline**

State information systems are connected with one another and with those of third-party stakeholders and service providers, creating shared risk. In order to establish a common security baseline, Cyber Security Services has defined a minimum set of controls, based on the Center for Internet Security (CIS) Controls, https://www.cisecurity.org/controls/.

All agencies must, at minimum, implement the CIS Controls - Basic, as defined in CIS Controls Version 7, by June 2021. These controls are:

- Inventory and Control of Hardware Assets.
- Inventory and Control of Software Assets.
- Continuous Vulnerability Management.
- Controlled Use of Administrative Privileges.
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.
- Maintenance, Monitoring and Analysis of Audit Logs.

The CSS will provide guidance and assistance to agencies on meeting these controls.

These controls establish minimum requirements for all agencies, but are not a comprehensive set of all activities required to protect agency information assets. Agencies remain responsible for taking all necessary steps to secure agency information assets and for implementing statewide standards. Additionally, agencies should seek to implement all 20 CIS Controls as soon as practical.

(3) **Reviews and Updates**

The information security risk environment is constantly changing as new technology and services emerge. Consequently, the CSS will review this policy annually and update it, at a minimum, every two years to address evolving risks to state information assets.