ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE POLICY

NUMBER	SUPERSEDES
107-004-052	Policy #107-004-052 | 2020
EFFECTIVE DATE February 17, 2026 **REVIEWED DATE** December 2, 2025	**PAGE NUMBER** Pages 1 of 5

DIVISION

Enterprise Information Services (State CIO)

POLICY OWNER

Cyber Security Services

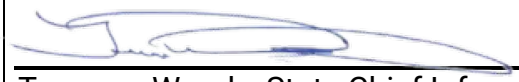
REFERENCE

- ORS 276A.300, 276A.303, 276A.306, 276A.323, 276A.326, 276A.329, 276A.332, 276A.335
- OAR 125-800
- Cyber and Information Security Procedure 107-004-052_PR

SUBJECT

Cyber and Information Security

APPROVED SIGNATURE



Terrence Woods, State Chief Information Officer

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

- Statewide Information Security Plan
- Statewide Information Technology Control Standards
- Human Risk Management Information Security Awareness and Training Program Plan
- Information Security Incident Response Plan
- Cyber Security Services Assessment Schedule

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.

Cybersecurity: the process of protecting information by preventing, detecting and responding to attacks.

Information security incident: a single or series of unwanted or unexpected information security event(s) 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 security event: an observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

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.

Offshoring: work performed or hosted wholly or in-part by companies proposing/assigning employees or contractors for state of Oregon work, who are not United states citizens or individuals without a valid United States visa (not authorized to work in the USA.

Users: agency, board, and commission full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities (subcontractors), 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.

SPECIAL SITUATIONS

State agencies unable to comply with the standards or procedures supporting this policy or cyber and information security program requirements must document the non-compliance and compensating controls and risks assessment and transmit to the State Chief Information Security Officer (CISO) at EIS.INFO@das.oregon.gov. Cyber Security Services (CSS) will review non-compliance transmittals to assess impact on enterprise risk and provide additional recommendations and requirements as appropriate.

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 must 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) **EIS – Chief Information Security Officer:**

The State CISO manages the state's information security program and serves as the CSS Director. 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 Technology Control 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.
- Implementing Statewide Information Technology Control Standards to effectively limit cyber and information security risks to agencies' business goals and objectives and state information assets.
- Managing and executing the enterprise cyber and incident response program.
- Managing the enterprise information security awareness and training program.
- Providing information to and coordinating information sharing among state agencies regarding cybersecurity 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.

(b) **Agencies:**

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 reducing cybersecurity risk exposure and ensuring the agency's activities do not introduce undue cybersecurity 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 statewide policies, standards, initiatives, and plans and with applicable federal and state laws and regulations. Plans include but are not limited to the Statewide Information Security Program Plan, Human Risk Management Information Security Awareness and Training Program Plan and Information Security Incident Response Plan.

The basic agency cyber and information security program requirements include:

- Confirming responsibilities for cyber and information security management between the agency and EIS.
- 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, as detailed in the Statewide Policy 107-004-010, Information Technology Asset Inventory and Management.
- Assessing threats, vulnerabilities and risks to agency information assets.
- Implementing Statewide Information Technology Control Standards to effectively limit cyber and information security risks associated with the agency's business goals and objectives.
- Establishing processes for information security incident identification and reporting, as outlined in the Information Security Incident Response Plan.
- Implementing security education, training and awareness for all users of agency information assets.
- Providing information security policies for agency users in a form that is relevant, accessible and understandable.

Each agency must comply with the Statewide Information Security Plan, statewide policies and security standards. 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 and procedures in accordance with the Statewide Information Security Plan and the Statewide Information Technology Control Standards.

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, 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**:

All users are governed by and responsible for complying with policies, plans, standards and guidance for information security, 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.
- 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, EIS has developed the Statewide Information Technology Control Standards which define baseline security controls for all systems.

Agencies must meet the Statewide Information Technology Control Standards.

CSS will provide guidance and assistance on meeting the controls.

(3) **CSS Assessments**

CSS will assess agency security posture using industry-standard metrics and methodologies (such as those developed by the Center for Internet Security) on the schedule posted on Guidance for State Agencies page of the CSS website. Agencies will ensure any findings identified in the assessment are remediated in accordance with the assessment recommendations.

(4) **Offshore and Foreign Services**

Offshoring computing services, to include, but not limited to cloud/hosting, application development, systems/service maintenance, and support is not allowed. Work performed or hosted wholly or in-part by companies proposing/assigning employees or contractors for state of Oregon work, who are not United States citizens or individuals without a valid United States visa (not authorized to work in the USA), is not permitted. Agencies may request an exception review from the State Chief Information Officer (CIO) for the following:

a) The agency does not receive solicitation responses or does not find an existing contract agreement proposing computing services hosted in the United States or qualified employees or contractors who are authorized to work in the United States. The company must provide an explanation regarding the need to use offshore computing services or employees or contractors not authorized to work in the United States in order to complete the contract or statement of work for the state of Oregon and disclose what policies are in place to mitigate data and security risks.
b) The agency director has declared an emergency and must solicit for critical services from companies who may offer computing services outside the United States or use employees or contractors not authorized to work in the United States to complete a state of Oregon contract or statement of work, in an emergency capacity. The company must disclose what policies are in place to mitigate any data and security risks associated with offshoring work.

Exception requests must be reviewed and approved by the State CIO prior to procuring. EIS may consult with the Oregon Department of Justice and other regulatory agencies before rendering a decision.

Agencies currently under contract or service agreements with a vendor who is hosting services outside the United States or is utilizing employees or contractors not authorized to work in the United States, to perform State of Oregon work, must submit those use cases to the State CIO for consideration and approval of continued use.