

Statewide Information Security Standards

Standards Category: Information Security

Title: Statewide Information System Development Lifecycle Standards

Number: S-107-04.8-10

Applicability: This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

Status: Adopted Draft Other: PENDING

Dates: (Effective Dates/Revisions/Reviews)

Effective: N/A Revisions: N/A Scheduled Review by: N/A

Prepared by: DAS Enterprise Information Strategy and Policy Division (EISPD)

Adopted by: _____
Dugan Petty, State Chief Information Officer Date

Statutory Authority: ORS 182.122

Enterprise Standard:

Minimum -

4.8. Information System Development Lifecycle Standards:

- 4.8.1 Access to operating system, source code, and operational or production application software/program directories, locations, and configuration files shall be managed, limiting access to authorized individuals.
- 4.8.2 When developing or modifying information systems, a change control management process shall be used to require authorization to initiate or make changes to the system, test and accept the changes, and move changes into production.
- 4.8.3 New or updated information system shall include adequate system documentation and ensure that system documentation is readily available to support the staff responsible for operating, securing and maintaining new and updated information systems.
- 4.8.4 Procurement of information systems designed to store, access or in any way handle information classified at level 3 or level 4 shall include requirements that information located on or transferred to or from these systems can be encrypted in accordance with the Encryption Standards in section 4.4.

Recommended -

4.9. Information System Development Life Cycle Recommended Best Practices:

- 4.9.1 Separate development, test and production environments should be used to protect production systems from development work and testing.

- 4.9.2 Segregation of duties between system developers and operations should be maintained, including between the following roles: system administration and system auditing; system development and system change; system operations and system security administration.
- 4.9.3 The early steps in the SDLC process through implementation are closely tied to the stages of project management as outlined in the Project Management Book of Knowledge (PMBOK), the state of Oregon's designated approach to project management. Key tasks should be considered for each step of the Information Security SDLC as defined by the National Institute of Standards and Technology (NIST) in the SDLC web site and brochure (<http://csrc.nist.gov/groups/SMA/sdlc/index.html>).

Section (1) - Purpose and Objective: The goal of information systems acquisition, development and management is to ensure that security is an integral part of information systems. Information systems are defined in ORS 182.122 as "computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure." This section describes security standards and best practices for Emerging Technologies, Business Cases, Encryption, Patch Management, and Information Systems Development Lifecycle.

Section (2) – Agency Deviations: In circumstances where the standards can/will not be implemented, the agency director must sign the Statewide Information Security Plan and Statewide Information Security Standards Deviation Report documenting compensating controls have been applied to adequately protect the information or acceptance of risk. This report must be kept on file for review by auditors or during a security assessment.

Section (3) – Standards Review: This standard will be reviewed at least ever two years after adoption and updated as needed.