ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

STATEWIDE POLICY

	NUMBER 107-004-050	**SUPERSEDES** Policy #107-004-050| January 1, 2008
	EFFECTIVE DATE 7/12/2023 **REVIEWED DATE** 7/12/2023	**PAGE NUMBER** Pages 1 of 4
Division **Enterprise Information Services (State CIO)**	**REFERENCE** ORS 162.305, 192.660, 276A.200, 276A.206, 276A.300, 291.110 OAR 125-800-0005, 125-800-0020	
Policy Owner Data Governance and Transparency		
SUBJECT Information Asset Classification Policy	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer (Signature on file with Strategic Initiatives and Enterprise Accountability Office)	

PURPOSE

This policy defines Oregon state government's approach to identifying, classifying, and protecting state data and information assets throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. For the purpose of this policy, data is incorporated into the definition of "information."

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

FORMS/EXHIBITS/INSTRUCTIONS

The Statewide Information Security Plan identifies information asset protection safeguards and the Statewide Information Security Standards define the minimum technical requirements and approaches for implementing these safeguards. The current version of each document can be found on the EIS Cyber Security Services page.

Enterprise Information Services' (EIS) Data Governance Policy (107-004-160) establishes the roles and responsibilities associated with stewarding data and information assets.

DEFINITIONS

Asset: Anything that has value to the organization. (Source: NIST Glossary)

Availability: Ensuring timely and reliable access to and use of information. (Source: NIST Glossary)

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Source: NIST Glossary)

Data: Unprocessed facts, raw numbers, figures, images, words, sounds, derived from observations or measurements. Data is the raw material for information. (Source: EIS Data Governance Policy)

Information: Data that has been processed to add context, meaning, and/or interpretation. Information assets may be documents, reports, analytical products, dashboards, or other products and exists in both digital and analog forms.

GENERAL INFORMATION

As with other assets, not all data and information assets have the same value or importance to the state and therefore information requires different levels of protection. Information asset classification is a critical first step to ensure that the state's information assets have a level of protection corresponding to their sensitivity and value. All state agency information must be classified and protected based on its confidentiality and sensitivity requirements.

Agencies comply with this policy by identifying information assets under the custodianship of the agency and subsequently assigning a classification level to each asset. Agencies should focus initially on identifying and classifying Level 3 or Level 4 information assets. Agencies may create procedures, standards or guidance consistent with this policy and the Statewide Information Security Standards. Agencies are expected to maintain information asset inventories and update them periodically. EIS may request an audit of the agency's established information asset inventory, classification program, or processes and procedures for inventorying and classifying information assets.

Information Classification Responsibilities

Each agency must establish procedures and practices for managing information assets within the agency's lines of business. These procedures and practices must:

1) Establish processes for identifying agency information assets and assigning classification levels;
2) Establish procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;
3) Ensure the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities, or changes in the environment;
4) Establish practices for periodic reclassification based on business impact, changing business priorities or new laws, regulations, and security standards; and
5) Establish practices in accordance with all laws and regulations for releasing or sharing information assets according to their classification level.

Information Classification Levels

Each agency shall identify its information assets and their sensitivity according to the classification scheme identified below. All information assets shall be classified strictly according to their level of sensitivity as follows:

Level 1, "Published" – Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients and partners. This includes information regularly made available to the public via electronic, verbal or hard copy media.

Examples: Press releases, brochures, pamphlets, public access webpages, and materials created for public consumption.

Level 2, "Limited" – Potentially sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients or partners. Agency shall follow its disclosure policies and procedures before providing this information to external parties.

For user account credentials (e.g. usernames and/or passwords) for state-owned or controlled information systems, agencies shall classify "personal information" as defined in ORS 646A.602(12)(a)(B) ("[a] user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification.") at a minimum as Level 2 information, unless criteria for a Level 3 or Level 4 classification for the related account or system also applies. If the related account or system contains Level 3 or Level 4 information, the user account information should be similarly classified.

Examples: Statewide risk management planning documents, published internal audit reports, email (may be Level 3 based on content), names and addresses that are not protected from disclosure.

Level 3, "Restricted" – Sensitive information, or regulated data intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency (for example, confidentiality/non-disclosure agreement) prior to receiving it.

Agencies shall classify "personal information" as defined in ORS 646A.602(12)(a)(A), at minimum as Level 3 information. Agencies shall classify "personal information" as Level 4 if the information meets the definition of Level 4 provided below.

Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as any violation of privacy practices, statutes or regulations. Information accessed by unauthorized individuals could result in financial loss or identity theft. Security efforts at this level are rigorously focused on confidentiality, integrity, and availability.

Examples: Network diagrams, personally identifiable information (for example, credit card information, Social Security numbers, regulated data), other information exempt from public records disclosure.

Level 4, "Critical" – Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

Examples: Information that, if disclosed, could result in loss of life, disability or serious injury or disruption to critical agency operations; regulated information with significant penalties for unauthorized disclosure.

Information may have different classifications during its life cycle. Agencies are responsible for periodic reclassification based upon business impact, changing business priorities and/or new laws, regulations, and security standards. Information received from another agency must be maintained according to the classification assigned by the custodian agency.