DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Policy

SUBJECT:	Information Asset Classification	**NUMBER:**	107-004-050
DIVISION:	Enterprise Information Strategy and Policy	**EFFECTIVE DATE:**	01-31-08

APPROVED: Kris Kaub

POLICY/ PURPOSE:

Purpose: The purpose of this policy is to ensure State of Oregon information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the agency and therefore information requires different levels of protection. Information asset classification and data management are critical to ensure that the state's information assets have a level of protection corresponding to the sensitivity and value of the information asset. This policy collectively applies to all information assets, including but not limited to paper, electronic and film.

Policy: All state agency information will be classified and managed based on its confidentiality, sensitivity, value and availability requirements. Each agency will identify and classify its information assets. Proper levels of protection will be implemented to protect these assets relative to the classifications. This policy is subject to the limitations and conditions of the Oregon Public Records Law.

Information Ownership

All information will have an information owner or owners established within the agency's lines of business. Owners can be individuals or groups of individuals as best meets the business model of the agency. The information owner(s) will be responsible to:

- Create an initial information classification, including assigning classification levels to all data;
- Approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management;
- Ensure the information will be regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities, or changes in the environment.
- Perform periodic reclassification based upon business impact analysis, changing business priorities and/or new laws, regulations and security standards.
- Follow state archive document retention rules regarding proper disposition of all information assets.

When a person(s) designated as information owner no longer has this responsibility due to departure, transfer or reassignment of duties, the agency will appoint a new information owner(s) in a timely manner to ensure no lapse in accountability and responsibility for information assets.

Asset Classification Levels

Each agency shall identify its information assets for the purpose of defining its value,

criticality, sensitivity and legal implications. Agency must use the classification schema included in this policy to differentiate between various levels of sensitivity and value. 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 Web pages, and materials created for public consumption.

- **Level 2, "Limited"** – 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, partners. Agency shall follow its disclosure policies and procedures before providing this information to external parties.

  Examples: Enterprise risk management planning documents, published internal audit reports, names and addresses that are not protected from disclosure.

- **Level 3, "Restricted"** – Sensitive information 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.

  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, 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: Disclosure that could result in loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure, information that is typically exempt from public disclosure.

Information Asset Protection

Each information asset classification will have a set or range of controls, designed to provide the appropriate level of protection of the information commensurate with the value of the information in that classification.

Compliance

Agencies will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Oregon Consumer Identity Theft Protection Act (Senate Bill 583, 2007 Legislative Session) as they relate to personal information.

Each agency may, based upon its individual business needs or legal requirements, exceed the security requirements put forth in this policy but must, at a minimum, achieve the security objectives defined in this policy.

To reduce the state's risk exposure for information not covered under Senate Bill 583, agencies will focus initially on classifying and protecting Level 4, "Critical" information. Classification of information shall be accomplished in accordance with the following timeline:

- Agencies shall develop a plan for identifying, classifying and protecting information assets. The plan will be in place no later than June 30, 2009.
- All Level 4, "Critical" information assets will be identified and protected no later than December 31, 2009.
- Agencies shall comply with all other provisions of this policy, including identification, classification and protection of all information assets, by June 30, 2010.

AUTHORITY: This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

ORS 162.305	Tampering with public records
ORS 192.501	Public records conditionally exempt from disclosure
ORS 192.502	Other public records exempt from disclosure
ORS 192.660	Executive sessions permitted on certain matters; procedures; news media representatives' audience; limits
ORS 291.037	Legislative findings on information resources
ORS 219.110	Achieving Oregon benchmarks; monitoring agency progress

Statewide Policy

POLICY NAME: Information Asset Classification **POLICY NUMBER:** 107-004-050

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.

ATTACHMENTS: None.

DEFINITIONS:

Asset: Anything that has value to the organization.

Availability: The reliability and accessibility of data and resources to authorized individuals in a timely manner.

Classification: A systematic arrangement of objects into groups or categories according to a set of established criteria.

Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information Owner: A person or group of people with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security: Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

Sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

GUIDELINES:

Information Asset Classification Responsibilities

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

- Establish processes for identifying agency information assets and assign classification levels to all data;
- Establish procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;
- 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;
- Establish practices for periodic reclassification based on business impact analysis, changing business priorities or new laws, regulations and security standards; and
- Enforce state archive document retention rules regarding proper disposition of all information assets.

Labeling Limited, Restricted or Critical Information

Proper labeling enables all parties to correlate the information with the appropriate information handling guidelines. Information should be properly labeled so that users are aware of classification.

The key to effective labeling is ensuring that a person with access to the information is aware of its classification and what restrictions exist in the release or handling of the information. Each individual piece of information or data does not necessarily have to be physically labeled. For example, one alternative to specifically labeling "Published" information is to have an agency policy that states "Published" information has no label on it while "Limited," "Restricted" and "Critical" are specifically labeled. In this case, agency staff would know that a particular piece of information is at the "Published" level because the information is not labeled.

Information labeling can also occur at a higher or aggregate level than the specific data or document level, depending on how the information is accessed. For example, it may be more effective to label information at the folder level, screen level, application level, report level, or form level, than at the specific document level or data field level. Any labeling strategy that effectively alerts the person accessing the information about its classification level would comply with this policy.

Information Handling

The state's information assets should be handled in a manner to protect the information asset from unauthorized or accidental disclosure, modification or loss. All information assets should be processed and stored in accordance with the information asset classification levels assigned in order to protect the confidentiality, integrity, availability, and level of sensitivity.

An agency that uses information from another agency should observe and maintain appropriate security for the classification assigned by the owner agency.

Information Isolation

Information belonging to different information asset classifications should be logically or physically separated or the aggregate information protected at the highest classification level. Whenever and wherever possible, information assets classified as "Critical" should be stored in a separate, secure area.

Proper Disposal

All electronic, paper and physically recorded information assets should be disposed of in a manner consistent with the information asset classification of the information and

comply with established State of Oregon archive laws, rules and regulations. For disposal of electronic equipment, refer to Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).