

Oregon Public Employees Retirement System	Posted date October 21, 2010	Number 1.10.01.01.003.POL
Signature <i>Paul N. Cleary</i>	Approval date October 21, 2010	Page 1 of 7
Policy:	Data Classification	
Objective:	Ensures information assets are identified, properly classified, and protected throughout their lifecycles.	
Reference:		

Policy

Information, like other assets, must be properly managed from creation to disposal. As with other assets, not all information has the same value or importance to the agency; therefore, information requires different levels of protection. Information asset classification and data management are critical to ensure 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. All employees are responsible for maintaining the confidentiality, integrity, and availability of the agency's information assets according to this policy.

All information will be classified and managed as outlined in this policy based on its confidentiality, sensitivity, and value. Each division will identify and classify its information assets. Proper levels of protection will be implemented to protect these assets relative to their classification. This policy is subject to the limitations and conditions of Oregon public records law Oregon Revised Statute (ORS) 192.

Authority

Department of Administrative Services (DAS) Information Asset Classification policy [107-004-050](#).

Definitions

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

Personally Identifiable Information (PII): As defined by ORS 646A.602(11), personal information means:

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

(a) Consumer's first name or first initial and last name in combination with any one or more of the following data elements when the data elements are not rendered unusable through encryption, redaction, or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) Social Security number;

(B) driver's license number or state identification card number issued by the Department of Transportation;

(C) passport number or other United States issued identification number; or

(D) financial account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a consumer's financial account.

(b) Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction, or other methods if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.

Redaction: Means removing portions of a data element to make it unrecognizable or incomplete. Methods of redaction usually consist of only showing the last four digits of a person's SSN or account number or using some form of black highlighter or other method to obscure that portion of information one is trying to protect from disclosure.

Default Classification Level

Information that is not labeled and cannot be easily identified as Level 1 should be handled as described in this document for Level 2.

Classification Levels

Information owners shall identify information assets for the purpose of defining the level of sensitivity. Divisions 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:

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

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, or 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, or partners. The agency shall follow its disclosure policies and procedures before providing this information to external parties.

Examples: Enterprise risk management planning documents, names, and addresses that are not protected from disclosure, such as work address, work email address, work phone numbers, etc.

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. The agency shall follow its disclosure policies and procedures before providing this information to external parties.

Examples: Sensitive internal management documents such as budget development documents, Network diagrams, personally identifiable information, or any information that can be directly tied to a member, such as PERS ID numbers, SSN (redacted or not), address, telephone number, email address, etc. Does not apply to work address, work email address, work phone number, etc.; documents with completed member information; screen prints; disability information; security audit reports; and any information exempt from public records disclosure (see ORS 192.501 and ORS 192.502).

Level 4, Critical – Information 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. The agency shall follow its disclosure policies and procedures before providing this information to external parties.

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

Examples: Disclosure that could result in loss of life, disability or serious injury, and information that is typically exempt from public disclosure. The agency does not usually maintain Level 4 information.

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. Information that is aggregated must be protected at the highest classification level. Refer to the Information Handling Standards document for the appropriate protection methods of each classification level.

Level 1 data does not require special handling or safeguards.

Level 2 data must have reasonable safeguards such as filing in a drawer or other area and not readily viewed by the public. Level 2 data may be sent electronically or mailed without special security controls at the discretion of the information owner.

Level 3 data should always be kept locked in a secure location. Multiple layers of protection such as a secure building, access control, and locked offices within a building are adequate protection. Electronic transmission of Level 3 data with PII must be secured via encryption or secured form of transport. Disclosure, transmission, or dissemination of Level 3 data must be authorized by the information owner.

Level 4 data must always be kept locked in a secure location (e.g., cabinet, safe, etc.). Electronic transmission of Level 4 data must be secured via encryption and such safeguards as digital certificates. Disclosure, transmission, or dissemination of Level 4 data must be authorized and documented by the executive director, deputy director, or a division administrator. Whenever and wherever possible, information assets classified as Level 4 - Critical should be stored in a separate, secure area.

Compliance

Information owners may, based upon individual business needs or legal requirements, specify security requirements that exceed those put forth in this document but must, at a minimum, achieve the security objectives defined in this policy.

The agency shall properly identify and protect information meeting the definitions, requirements, and effective dates outlined in the Oregon Consumer Identity Theft Protection Act ORS 646A.600 and DAS Information Asset Classification policy [107-004-050](#).

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

Information owner responsibilities

The deputy director owns all enterprise systems such as jClarety, FileNet, and RIMS. The deputy director delegates authority to division administrators to manage access to specific program areas. Division administrators delegate management of specific business processes to section managers.

The systems are designed to allow access by role. Only those employees assigned a role can access data needed to complete their assigned tasks.

Ad-hoc reports developed through these systems are owned by the section manager from which the report was created.

Information owners are responsible for:

- establishing processes for identifying information assets and assigning classification levels to data;
- establishing procedures in support of decision making regarding controls, access privileges of users, and ongoing information management;
- ensuring the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities, or changes in the environment;
- establishing practices for periodic reclassification based on business impact analysis, changing business priorities or new laws, regulations, and security standards; and
- enforcing state archive document retention rules regarding proper disposition of all information assets.

Labeling

Labeling is an aid that helps enable all parties to correlate the information with the appropriate information handling standards. Information should be properly labeled so users are aware of its classification.

Information that is classified at Level 1 is not to be labeled. Information that is classified at Levels 3 and 4 must be labeled. To help differentiate between Level 1 and Level 3, information classified at Level 2 might be labeled.

All labels should use the preferred three character code as follows:

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

SL2 for Level 2 – Limited information

SL3 for Level 3 – Restricted information

SL4 for Level 4 – Critical information

Labels are to be placed on the bottom left portion of the document when possible. For example, Word and Excel documents should contain the label in the bottom, left footer. The preferred labeling schema is SL2, SL3, or SL4 (all caps) without spaces, additional wording, or notations.

Labels for e-mail (internal and external) should be in the e-mail's signature. Any person that sends, replies, or forwards an e-mail to another is the owner of that e-mail and is required to ensure the appropriate label is used.

When sending email to a mailbox outside of the PERS email system (i.e., contractor, employer, member, DAS, vendor, etc.), you must add a confidentiality note to the email. The verbiage to use is:

Confidentiality Note: *All information in this email, including attachments, is approved solely for delivery to and authorized use by intended recipients. Use, dissemination, distribution, or reproduction of this message and/or any of its attachments by unintended recipients is not authorized and may be unlawful. If you are not an intended recipient of this message or an authorized assistant to an intended recipient, please notify the sender by replying to this message, and then delete it from your system.*

Labeling electronic files poses additional challenges and should be named in some manner that complies with these labeling requirements so the user does not need to open a file to determine its classification. As an example, a file containing Level 3 information could be named SL3_filename.ext.

Management may also choose to store like-classified documents in a network folder named using the above labeling three-character code such as SL3_Files or methods similar that comply with the intent of this policy. If a file is moved from this location, renaming the file should be considered.

If users have any questions concerning these guidelines, they should contact their immediate supervisor, the agency Records Officer, Information Security Officer, or ISD Administrator.

Information Handling

Information assets must be handled in a manner that protects the information asset from unauthorized or accidental disclosure, modification, or loss. All information assets should be processed and stored

Origination date: September 6, 2005

Last revision date: October 19, 2010

Last review date: October 19, 2010

SL2

in accordance with the information asset classification levels assigned to protect the confidentiality, integrity, availability, and level of sensitivity. Refer to the Information Handling Standards document.

Information coming from outside the agency's control should be properly classified by the originating source. PERS shall treat such information received with the appropriate level of protection based on the originating owner's classification. Management can determine a higher level of classification if it is appropriate. If the originating organization has not clearly labeled or classified this information, PERS will assess the information and treat the information as defined in this policy.

Proper Disposal

All electronic, paper, and physically recorded information assets must be disposed of in a manner consistent with the classification of the information asset and comply with all established state of Oregon archive laws, rules, and regulations. For disposal of electronic equipment, refer to the DAS Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery) policy [107-009-0050](#).

Additional resources

- [Information Handling Standards](#)
- [Release of Sensitive Information policy 1.01.00.00.028](#)

Origination date:	September 6, 2005
Last revision date:	October 19, 2010
Last review date:	October 19, 2010