State of Oregon
OREGON DEPARTMENT OF EDUCATION
# POLICY MANUAL

AGENCY POLICY 581-309

Effective Date: 03-03-2010
Revised Date: 03-21-2021

**APPROVED: Signature on File at ODE**

**RE: Information Asset Classification**

## Purpose
The purpose of this policy is to ensure that the Oregon Department of Education (ODE) information assets are identified, properly classified, and protected throughout their life cycles. 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 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, transported and stored data.

## Policy
All ODE information assets will be classified and managed based on the data confidentiality, sensitivity, value and availability requirements. Each ODE office shall identify and classify its information assets to determine security controls for protection and use of its data. Proper levels of protection will be implemented to protect these assets relative to the classifications. Offices are responsible for implementing appropriate managerial, operational, physical and technical controls for access to, use of, the transmission of, and the disposal of data assets in compliance with this and related ODE and State policies. This policy is subject to the limitations and conditions of the Oregon Public Records Law.

## Authority
Department of Administrative Services (DAS) Statewide Policy # 107-004-050, Information Asset Classification and DAS Statewide Policy # 107-004-100, Transporting Information Assets.

## Applicability
This policy applies to all ODE information assets and to all ODE employees, contractors, and volunteers.

## Definitions for this policy

**Asset:** Anything that has value to the organization.

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

**Breach:** A loss of confidentiality, integrity or availability that has the potential to cause some level of negative impact to the agency.

**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 documented material, regardless of its physical form or characteristics.

**Information Asset:** Information relevant to an agency's business function, including captured and tacit knowledge of employees, customers or business partners; data and information stored in highly-structured databases; data and information stored in textual form and in less-structured databases such as messages, e-mail, workflow content and spreadsheets; information stored in digital and paper documents; purchased content; and public content from the Internet or other sources.

**Information/Data Owner:** A person or group of people with authority for specified information and responsibility for classifying that information for use and 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 measure of the trustworthiness of information and systems. A security principle that makes sure that information and systems are not modified maliciously or accidentally.

**Personally Identifiable Information (PII):** As defined by ORS 646A.602(11) "Personal information":

(A) Means 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 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, 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) Means 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.

(C) ODE PII includes additional data elements not identified by ORS 646A.602(11), when combined with a child, youth or student's (age birth to 24) first, last name including (but not limited to):
   a) Student Secure ID (SSID)
   b) Birthdate
   c) Socio-Economic Status
   d) English Learner Status
   e) Special Education Status and/or Disability Information

**Sensitive Information:** Any information, the loss or misuse of which could adversely affect 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.

**Asset Classification Levels**

Asset Classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the ODE should that data be disclosed, altered, or destroyed without authorization. All ODE formal collections require classification levels. Information/Data Owners shall identify information assets for the purpose of defining their value, criticality, sensitivity and legal implications. In addition, for offices without formal data collections that collect or use data, offices must use the classification schema included in this policy to differentiate between various levels of sensitivity and value, and apply the level of security controls necessary to secure the data from breach or unauthorized use.

**Default Classification**

Information that is not labeled and cannot be easily identifiable as Level 1, should be handled as described in this document for Level 2.
All information assets shall be classified strictly according to their level of sensitivity and value 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 students, children, 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, names and addresses that are not protected from disclosure. This applies to public staff directories and student directory information.

> **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, students, 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 ODE job 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. All "Level 3" data requests must be approved by the ODE Data Governance Committee.

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.

Level 3 data must be protected at rest, in transport, and during use. This level of data must not be sent to individuals through email. Level 3 data should not be stored outside of ODE secured databases unless other security controls are in place. To store Level 3 data outside a secured database, a password protected network drive must be created.

For transport or necessary sharing of Level 3 data, ODE employees, contractors, and agents must use the ODE "secure file transfer" application or work with ODE IT staff to receive an FTP for use.

*Examples:* Student Information, Assessment Test Materials, Network diagrams, Personally Identifiable Information, completed retirement applications, documents and

spreadsheets or screen-prints containing SSN and name, employee and retiree address, telephone and other nonfinancial membership records and employee financial records maintained by ODE, disability information, security audit reports, aggregate data where appropriate suppression has not been applied, and other information exempt from public records disclosure.
*Student Education Records are also protected by FERPA*

> **Level 4, "Critical" –** Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is 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, information that is exempt from public disclosure. The ODE does not usually maintain Level 4 information, however if a student or staff is in protective custody, a restraining order has been executed, or other legal systems have restricted the access to their records, their PII can be considered Level 4 due to the harm that disclosure could cause the individual(s).

**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. Refer to the Information Handling Standards Matrix (Appendix A) for the appropriate protection methods of each classification level.

Level 4 data must always be kept locked in a secure location (e.g., cabinet, safe, etc.). Multiple layers of protection such as a secure building, access control, and locked offices within a building are required for this level of data. 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 ODE Director along with the ODE Legal Department.

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 must be secured via encryption or a secured form of transport. Disclosure, transmission or dissemination of Level 3 data must be authorized by the data owner, or the Data Governance Committee. In situations where subpoenas have been received the ODE Legal department may also release Level 3 data, using secured transport.

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 1 data does not require special handling or safeguards.

**Compliance**

Information/Data 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 document.

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 to 646A.628) and statewide Department of Administrative Services (DAS) Policy 107-004-050, Information Asset Classification.

### Information/Data Owner Responsibilities

The ODE Agency Director is responsible for all enterprise systems and information assets. The Agency Director delegates authority to Assistant Superintendents to manage access to specific program areas. Assistant Superintendents delegate management of specific business processes to Directors. Directors oversee data ownership within their specific supervision and therefore are accountable for enforcing policy.

All ODE systems are designed with role-based security for access. Only those employees assigned a role can access data needed to complete their assigned tasks.

Information/Data 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 and destruction of information assets.

### Labeling 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.

Information classified at Levels 3 and 4 must have specific labeling.

In order to ensure a consistent implementation of the agency's document labeling practice as required by this Policy, the following guidelines should be used when labeling agency documents.

All documents created by agency staff that include Level 3, and Level 4 data need to contain a classification label. This includes reports, spreadsheets, letters, memos, etc.

All labels will be a two character code as follows:

Use **L3** for Level 3 – Restricted information
Use **L4** for Level 4 – Critical information

Labels are to be placed on the bottom left portion of the document where possible. For example, Word, PDF and Excel documents should contain the label in the bottom left of the document footer.

If Users have any questions concerning these guidelines, they should contact their immediate supervisor, the Chief Information Officer (CIO), or the Data Governance Committee (DGC).

### Information Handling

Information assets must 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.

Information coming from outside the agency's control should be properly classified by the originating source; ODE 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 appropriate. If the originating organization has not clearly labeled or classified this information, ODE will assess the information and treat the information as defined by this policy.

### 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 must 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 DAS Policy 107-009-050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

### Additional Resources

ODE Policy 581-101 Handling Confidential Information
ORS 646A.600 to 646A.628

## PAGE LEFT BLANK ON PURPOSE

# Appendix A

## Information Handling Standards Matrix

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| **Criteria** | Information that can be made available to anyone without exception. It is neither sensitive nor controlled. | Information that management believes requires limitations on internal access on a "need to know" basis, but which does not fall under the definition of "Restricted" or "Critical." | Restricted information requiring special precautions be taken to ensure its accuracy, relevance, timeliness, and completeness.<br>This information, if lost, could cause significant financial loss, inconvenience or delay in performance of the agency's mission and loss of public trust. Student education records are protected by Federal law (FERPA) which requires reasonable methods of security controls. | Information that has limitations placed on its internal access and that may be disclosed only in accordance with an executive order, public law, federal statement, and supporting policies, guidelines, procedures, and processes. |

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| **Handling standards** | No special handling required | No special handling required | Restricted data must be handled securely at all times. This level of data must be protected from unauthorized use or access<br>This requires:<br>• Encryption for storage and transport<br>• Paper files be kept in locked cabinet or storage area<br>• Proper storage for electronic files (must NOT be stored on personal devices, laptops, tablets, PC's, etc.)<br>• Only authorized personnel can access | Critical data must be handled securely at all times. This level of data must be protected from unauthorized use or access. This data is extremely sensitive<br>This requires:<br>• Encryption for storage and transport<br>• Paper files be kept in locked cabinet or storage area<br>• Proper storage for electronic files (must NOT be stored on personal devices, laptops, tablets, PC's, etc.)<br>• Only authorized personnel can access<br>• Annual or bi-annual training be completed prior to authorization of access |
| **Release to third parties** | Available to the general public and for distribution outside of the agency | Intended for use only within the agency<br>• May be shared outside the agency only if there is a legitimate business need to know, and is approved by the data owner and director | Access is limited to as few persons as possible on a need to know basis<br>• Information is very sensitive and closely monitored using audit tools.<br>• Information is controlled from creation or acceptance to destruction or return of information.<br>• Release only permitted by appropriate policies and procedures.<br>• Requires Data Governance Committee approval | Access is limited to as few persons as possible on a need to know basis<br>• Information is very sensitive and closely monitored using audit tools.<br>• Information is controlled from creation or acceptance to destruction or return of information. Release only permitted by appropriate policies and procedures<br>• Requires legal department approval |

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| **U.S. Mail / Other Mail service** | No special handling required for inside and outside agency | • No special handling required for inside agency<br>• Outside agency, use 1st class mail | • Sealed interoffice envelope marked and labeled "sensitive information" Notify the recipient in advance<br>• Outside agency, 1st class trackable delivery is required | • Sealed interoffice envelope marked and labeled "sensitive information" Notify the recipient in advance<br>• Outside agency, 1st class trackable delivery is required |
| **Email** | No special handling required | No special handling required | Not allowed. Send via "secure file transfer" | Not allowed. Send via "secure file transfer" |
| **FAX** | Located in an area not accessible to the general public<br>Requires:<br>• Cover sheet<br>• Reasonable care in dialing | Located in an area not accessible to the general public<br>Requires:<br>• Cover sheet<br>• Reasonable care in dialing | Located in an area not accessible to the general public and unauthorized persons<br>Requires:<br>• Cover sheet labeled "Sensitive Information"<br>• Telephone notification prior to transmission and confirmation of receipt | Located in an area not accessible to the general public and unauthorized persons<br>Requires:<br>• Cover sheet labeled "Sensitive Information"<br>• Telephone notification prior to transmission and confirmation of receipt |
| **Transmission by spoken word** | No special precautions required | No special precautions required | Active measures and close control to limit information to as few persons as possible<br>Requires:<br>• Enclosed meeting area | Active measures and close control to limit information to as few persons as possible<br>Requires:<br>• Enclosed meeting area |

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| | | | • Avoidance of outside listeners<br>• No public places, announcements, speakerphones<br>• Landline phones are preferred | • Avoidance of outside listeners<br>• No public places, announcements, speakerphones<br>• Landline phone are preferred<br>• Authorized staff only |
| **Print, film, video standards** | No special precautions required | Reasonable precautions to prevent inadvertent disclosure<br>Requires:<br>• Printed materials be stored out of sight of non-employees<br>• Sign-in sheets/logs placed out of sight of non-employees<br>• Monitors positioned or shielded from non-employees | Active measures and close control to limit information to as few persons as possible<br>Requires:<br>• Printed materials be stored out of sight in lockable enclosure<br>• Sign-in sheets/logs not contain sensitive information<br>• Monitors positioned to prevent unauthorized viewing<br>○ Secure area<br>○ Password screensaver on short delay | Active measures and close control to limit information to as few persons as possible<br>Requires:<br>• Printed materials be stored out of sight in lockable enclosure<br>• Sign-in sheets/logs not contain sensitive information and other signers identity safeguarded<br>• Monitors positioned to prevent unauthorized viewing<br>○ Secure area<br>○ Password screensaver on short delay |
| **Copying** | No special precautions. | No special precautions. | Photocopying with approval of information owner.<br>Note: If a digital copier is used, cache needs to be erased | Photocopying with approval of information owner.<br>Note: If a digital copier is used, cache needs to be erased |

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| **Document/Data Storage** | • Printed material has no special precautions required<br>• Electronic documents can be stored on computer and all network drives<br>• Can be emailed both internally and externally | • Printed material requires reasonable precautions to prevent access by non-employees<br>• Electronic documents can be stored on computer and all network drives<br>• Can be emailed as long as reasonable precautions are taken to assure delivery to authorized person | • Printed material requires storage in a lockable enclosure<br>• Electronic documents must be stored on secure drives only. Password protected documents are preferred. Destruction rules apply<br>• Email is not allowed for transmission or storage of documents containing L3 data | • Printed material requires storage in a lockable enclosure<br>• Electronic documents must be stored on secure drives only. Password protected documents are preferred. Destruction rules apply<br>• Email is not allowed for transmission or storage of documents containing L4 data |
| **Destruction** | No special precautions required | No special precautions required | • Destroy in a manner that protects sensitive information<br>• Waste bins used must be in a secure area not accessible to unauthorized persons<br>• Paper recycling is prohibited unless labeled “for shredding”<br>• Computers, hard-drives, other devices and objects must be turned into IT for cleansing prior to reuse | • Destroy in a manner that protects sensitive information<br>• Waste bins used must be in a secure area not accessible to unauthorized persons<br>• Paper recycling is prohibited unless labeled “for shredding”<br>• Computers, hard-drives, other devices and objects must be turned into IT for cleansing prior to reuse |
| **Physical security** | • Workstations must be locked when unattended regardless of data classification | • Workstations must be locked when unattended regardless of data classification | • Workstations must be locked when unattended regardless of data classification | • Workstations must be locked when unattended regardless of data classification |

| | Level 1-Published | Level 2-Limited | Level 3-Restricted | Level 4-Critical |
|---|---|---|---|---|
| | • When printing documents, no special precautions required | • When printing documents, no special precautions required | • Laptops and other devices must be password protected and not left unattended in an unlocked area<br>• When printing or copying documents, user must immediately extract from printer / copier<br>• All PSB floors are locked, precautions must be taken to not allow unauthorized persons onto floors | • Laptops and other devices must be password protected and not left unattended in an unlocked area<br>• When printing or copying documents, user must immediately extract from printer / copier<br>• All PSB floors are locked, precautions must be taken to not allow unauthorized persons onto floors |
| **Audit** | None | None | • Access shall be granted by the information owner with appropriate access paperwork signed by auditor(s) | • Access shall be granted by the information owner with appropriate access paperwork signed by auditor(s) |