



OREGON YOUTH AUTHORITY
Policy Statement
Part I – Administrative Services



Subject:

Information Asset Classification and Protection

Section – Policy Number:

E: Information Management: 3.2

Supersedes:

I-E-3.2 (6/10)

Effective Date:

12/30/2014

Date of Last

Review:

12/23/2016

Related Standards and References:

- DAS, Statewide Policy [107-004-050](#), Information Asset Classification
- [OYA policy](#): I-E-2.1 (Public Records Requests for Agency Records)
 I-E-2.3 (Requests for Youth Records, Reports, and Other Materials)
 I-E-3.3 (Information Security Incident Response)
[I-C-9.0](#) (Mobile Communication Devices and Other Mobile Data Storage Devices)
- [JJIS policy](#): Confidential JJIS Information Exchanged Electronically
- [OYA Information Asset Classification and Protection Matrix](#)
- [Information Asset Classification Handling Guide](#)

Related Procedures:

- None

Policy Owner:

OYA Information Security Officer

Approved:


 Fariborz Pakseresht, Director

I. PURPOSE:

This policy sets guidelines for OYA staff in classifying and protecting information assets according to their risk levels.

For guidelines on responding to public or youth records requests, see OYA policies I-E-2.1 (Public Records Requests for Agency Records), and I-E-2.3 (Requests for Youth Records, Reports, and Other Materials).

II. POLICY DEFINITIONS:

Asset: Anything that has value to the organization.

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.

OYA Information Security Office (ISO): OYA employee who is responsible for overseeing the agency's information security program to help ensure the security objectives are addressed.

III. POLICY:

OYA identifies and classifies its information assets by risk level and ensures protection according to classification levels. This policy establishes how OYA information assets are identified, assigned classification risk levels, and what the protection standards are for the different classification levels.

IV. GENERAL STANDARDS:

A. Information Asset Classification

1. All information assets must be classified according to their level of sensitivity as follows:
 - a) **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 through electronic, verbal or hardcopy media.
 - b) **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. OYA must follow its disclosure policies before providing this information to external parties.
 - c) **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 prior to receiving it.
 - d) **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.

2. Each information owner must -
 - a) Identify the information they work with;
 - b) Determine what specific data is found within the information;
 - c) Assign a risk level to the information asset based on the specific data identified;
 - d) Inform the OYA Information Security Officer of the information asset and the risk level assigned to it; and
 - e) Implement the prescribed standard of protection and handling and communicate it to others who use or have access to the information asset.
3. As information assets are received, modified or eliminated, the same evaluation and reporting procedures listed above must occur.

B. Information Asset Classification Matrixes

1. All OYA information assets must be listed in an OYA Information Asset Classification matrix with instructions on how to protect and handle the information assets.
2. The OYA Information Security Officer must -
 - a) update the Information Asset Classification and Protection matrixes as information assets are classified by information owners;
 - b) set the standard of information asset protection and handling; and
 - c) coordinate a biennial review of the matrixes by all information asset owners to ensure the matrixes are current and match the agency retention schedule.
3. The OYA Information Asset Classification matrix and [Information Asset Classification Handling Guide](#) are accessible to all OYA staff.

C. Labeling

Level 3 -Restricted and Level 4 -Critical information must be specifically labeled so users are aware of the classification and may handle or release it appropriately according to information protection guidelines. Labels may be hardcopy, ink stamped, or electronic.

The following guidelines must be used when labeling OYA information in order to ensure consistency in the OYA's information labeling practice as required by this policy:

1. All Level 3 and Level 4 information created by OYA staff must have a classification label. This includes reports, spreadsheets, letters, memos, e-mail, etc.

Such labels must specify the level as “Restricted Information” or “Critical Information.”

2. Labels must be placed on the bottom of the document when possible. For example, Word and Excel documents may contain the label in the footer.

When this is not possible, a label must be placed on the file folder or cabinet/container where the document is stored.

3. Youth medical files must be clearly labeled as “Health Services Record” on the outside of each file folder. The cabinet/container where the medical files are stored must be labeled as “Restricted Information.”
4. Youth case file labels must be placed on the outside of the file folders. The cabinet/container where the youth case files are stored must be labeled as “Restricted Information.”

5. Labels must be placed on juvenile parole/probation officer (JPPO) “case notebooks” as follows: “Restricted Information. Please return to: (JPPO’s field office address).”

6. Labels for e-mail must be in the body of the email.

E-mail generated from within OYA’s email system will automatically contain the label as a default message.

7. Users may contact their immediate supervisors or the OYA Information Security Officer with questions concerning these guidelines.

D. Staff Training

New staff must be trained on this procedure during New Employee Orientation.

E. Compliance Monitoring

Compliance with prescribed protection standards will be evaluated when general program areas are audited or reviewed.

V. LOCAL OPERATING PROTOCOL REQUIRED: NO