DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Internal Operations Policy Manual

SUBJECT:	**Information Asset Classification and Transportation**	**NUMBER:**	**107-01-180**
DIVISION:	**Operations Division**	**EFFECTIVE DATE:**	**5/15/08**

APPROVED:

POLICY/ PURPOSE:

Purpose: The purpose of this policy is to ensure Department of Administrative Services 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 ensuring that the department's information assets have a level of protection that corresponds with the asset's sensitivity and value. This policy collectively applies to all information assets, including but not limited to paper, electronic and film.

Policy: All DAS information will be classified and managed based on its confidentiality, sensitivity, value and availability requirements. Each division 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.

AUTHORITY:

DAS Statewide Policy #107-004-050, Information Asset Classification
DAS Statewide Policy #107-004-100, Transporting Information Assets

APPLICABILITY: This policy applies to all DAS divisions and employees.

ATTACHMENTS: DAS Information Asset Classification Summary

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 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.

DEFINITIONS Continued:

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:

I. **Asset Classification Levels**

Each division shall identify its information assets for the purpose of defining its value, criticality, sensitivity and legal implications. 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:

- **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 and 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 disclosure, such as information covered under the Health Information Portability and Accountability Act or Internal Revenue Service regulations, information that is typically exempt from public disclosure.

II. Information Asset Protection

A range of controls will be designed for each level of information asset classification. Controls will be commensurate with the sensitivity of the information in each classification. This policy also provides guidelines for the transportation of sensitive assets; statewide policy 107-004-100 provides additional guidance on transporting information assets (see Operations Policies and Guidelines).

Level 4 data that exists in physical form (e.g. paper, thumb drives, CD, DVD, etc.) must always be kept locked in a secure location when not being used. A secure location is one that has at least two layers of control; these controls can include locked doors, locked file cabinets, and secure buildings. An example of two layers of control is a paper file secured within a locked file cabinet within a locked office or secure building.

Level 4 data that exists in electronic form (e.g., data bases, hard drives, statewide applications) must always be protected by two layers of control; these controls can include secure buildings, firewalls, encryption, or password protection.

Electronic transmission of level 4 data must be electronically safeguarded using such tools as encryption, password-protected zip files or digital certificates. Level 4 data sent by state shuttle must be secured in tamper-evident envelopes and tracked. Level 4 data sent by third party mail (e.g., USPS, UPS, etc.) may use standard processes unless the data owner determines a higher level of security is needed. The DAS Director, Deputy Director or Division Administrator must authorize disclosure, transmission or dissemination of level 4 data.

Level 3 data must always be protected by at least one layer of control when not being used; these controls can include a locked cabinet, desk or file drawer, a secure location such as within a locked office, behind firewalls, encryption, or password protection.

Electronic transmission of level 3 data may be electronically safeguarded using tools such as encryption, password-protected zip files or digital certificates if the data owner deems it necessary. Level 3 data sent by state shuttle may be secured in tamper-evident envelopes and tracked if the information asset owner deems it necessary. Level 3 data sent by third party mail may use standard processes unless the data owner determines a higher level of security is needed. The owner or designee of the information asset must authorize disclosure, transmission or dissemination of level 3 data.

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

Level 1 data does not require any special handling or safeguards.

III. Compliance

Divisions may, based upon individual business needs or legal requirements, exceed the security requirements put forth in this document but must, at a minimum, achieve the security objectives defined in this document. To reduce the state's risk exposure, divisions will focus initially on classifying and protecting Level 3, "Restricted" and Level 4, "Critical" information.

Notwithstanding the timelines outlined in this policy, divisions will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-628) as they relate to personal information.

Divisions have until December 31, 2008 to identify and protect information assets classified at Level 4, "Critical," except for personal information, which must be classified to meet the mandates of the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-628) by January 2008.

Divisions have until June 30, 2009 to identify and protect information assets that are classified at Level 3, "Restricted," except for personal information, which must be classified to meet the mandates of the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-628) by January 2008.

Divisions have until June 30, 2009 to identify and protect information assets that are classified at Level 2, "Limited."

IV. Information Asset Classification Responsibilities

Divisions are responsible for:

- Identifying the owners of each information asset;
- Establishing processes for identifying and inventorying division information assets and assigning classification levels to all 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.
- Ensuring that recipients of DAS-owned information assets understand the classification and handling requirements of each asset, understand the elements of this policy, and determine whether formal interagency agreements are needed when exchanging information assets.

V. 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 attachment "DAS Information Asset Classification Summary" shall be the document that identifies information classifications at all levels. Information classified at levels 3 and 4 must have specific labeling identifying the information as “restricted” or “critical”.

VI. 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 another agency should be properly classified by the originating agency; DAS recipients of such information must observe and maintain appropriate security for the classification assigned by the owner agency.

In accordance with Statewide Policies, recipients of DAS information assets must maintain appropriate security safeguards according to the classification level of the asset.

VII. 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.

VIII. 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.

Paper files containing level 3 or level 4 data must be disposed of so that confidentiality is maintained. Confidential shredding bins or shredding by staff are acceptable means of disposal.

For disposal of electronic equipment, refer to Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

IX. Additional Resources

A community of practice developed a set of resources to help agencies implement information asset classification. Those resources can be found at: http://oregon.gov/DAS/EISPD/ESO/IAC.shtml.