



# Information Asset Classification Security Policy

Subject <b>Information Asset Classification</b>	Approval Signature <i>Julie Ruthven</i>
Who this Policy Applies to <b>All agency employees</b>	Approval Date <b>9/26/2008</b>
Number <b>20.7.0</b>	Scheduled Review Date <b>9/26/2009</b>

---

## Purpose

The purpose of this policy is to ensure the Secretary of State's (Secretary) information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to its final 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.

Proper identification of information assets ensures assets will be classified by the Public Records Law. Improper identification of information assets may result in additional costs for legal interpretation and representation.

---

## 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.

**Controls:** Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

*- Focused on Security. Dedicated to Success. -*

**Encryption:** Process of converting information into an unintelligible form except to holders of a specific cryptographic key.

**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.

**Incident:** A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

**Information Owner:** Person with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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

**Personal Information:** 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:

- Social Security number
- Driver license number or state identification card number issued by the Department of Transportation
- Passport number or other United States issued identification number
- 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

**Risk:** The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

**Security Policy:** Documentation that describes senior management's directives toward the role that security plays within the organization. It provides a framework within which an organization establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and organization commitment managing risks.

*- Focused on Security. Dedicated to Success. -*

**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.

---

**Background** All agency information assets must be protected to ensure confidentiality, integrity, and availability of information from unauthorized use or modification and from accidental or intentional damage or destruction.

---

**Policy** All agency 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 which defines information as being open or exempt from public disclosure. See ORS 192.4.

- **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, Request For Proposals, Recruitment Announcements, Published Audit Reports, public access Web pages and Web database applications, and materials created for public consumption.

- **Level 2, “Limited”**

Sensitive information that will not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, partners. Divisions shall follow its disclosure policies and procedures before providing this information to external parties.

Examples: enterprise risk management planning documents, agency correspondence, petition signature sheets, performance evaluations,

*- Focused on Security. Dedicated to Success. -*

policies, names, regular and certified copies of business registry and UCC filings, and database extract reports, and addresses that are not protected from disclosure.

- **Level 3, “Restricted”**

Sensitive information intended for limited business use that is 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, customer financial account numbers (checking, debit, credit card, etc...), public records with unredacted personally identifiable information (social security numbers, driver license number, financial account numbers, etc...), public records qualified for personal safety exemption under ORS 192.445, Audit working papers, and other information explicitly exempt from public records disclosure by the Public Records Law is ORS 192.4.

- **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.

Each information asset classification will have a set or range of controls, designed to provide the appropriate level of protection of the information

*- Focused on Security. Dedicated to Success. -*

commensurate with the value of the information in that classification.

---

**Guidelines**      See ISO/IEC 27002:2005 for guidance

---

**References**      None