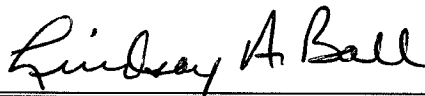


<b>SUBJECT:</b> Information Security	<b>NUMBER:</b> 107-004-052
<b>DIVISION:</b> Enterprise Information Strategy and Policy	<b>EFFECTIVE DATE:</b> 07/30/07
<b>APPROVED:</b> 	

**POLICY/  
PURPOSE:**

**Purpose:** Information security policies emphasize the state's commitment to information security and provide direction and support for information security in accordance with business requirements and relevant laws and regulations.

The ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. The International Standard ISO/IEC 27002:2005 was prepared to address information security. DAS has adopted the ISO 27002 standard to guide the creation of an enterprise information security policy set.

**Policy:** All agency information assets must be protected to ensure confidentiality, integrity, and availability. Each agency will develop and implement information security plans, policies and procedures that protect its information assets from the time of creation, through useful life and through proper disposal.

**Information Security**

Security is the ability to protect the confidentiality, integrity, and availability of information and to protect information assets from unauthorized use or modification and from accidental or intentional damage or destruction.

**Objectives**

Each agency, through its management, is required to protect and secure the information assets under its control. The basic information protection requirements include, but are not limited to:

- Compliance with applicable legislative, regulatory, and contractual requirements;
- Identifying information assets;
- Determining the value of information assets to the agency and the business processes they support;
- Assessing the vulnerability and risk associated with information assets;
- Providing the level of protection that is appropriate to the information assets' vulnerability, risk level, and agency value;
- Security education, training, and awareness for all users of agency information assets;
- Identification of general and specific responsibilities for information security management, including reporting information security incidents;
- Communication of information security policies throughout the agency to users in a form that is relevant, accessible and understandable.

**Roles and Responsibilities**

Each State Agency Head is responsible for information security in his/her

## Statewide Policy

**POLICY NAME:** Information Security

**POLICY NUMBER:** 107-004-052

agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. Each State Agency Head also is responsible for ensuring his/her agency's compliance with state enterprise security policies, standards, and security initiatives, and with state and federal security regulations.

All agency employees are responsible for protecting the confidentiality, integrity and availability of the agency's information assets.

### Planning

Each agency will establish a plan to initiate and control the implementation of information security within the agency and manage risk associated with information assets. The plan will include:

- Processes to:
  - Identify agency information assets;
  - Determine information sensitivity;
  - Determine the appropriate levels of protection for that information;
- Applicable state directives and legal and regulatory requirements;
- Identification of roles and responsibilities for information security within the agency;
- Identification of user security awareness and training elements; and,
- Information security policies that govern agency information security activities.

### Review and Evaluation

Protection of information assets is an ongoing process. Each agency will ensure that new business needs and risks are reflected in its information security plans and policies. Agency information security plans, policies, standards and procedures will be reviewed and revised, as needed, by the agency no less frequently than every five years.

### Compliance

Each agency may, based upon its 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.

State agencies have two (2) years from effective date of this policy to comply with this policy.

### **AUTHORITY:**

This policy is established under the authority of 2005 Oregon Laws Chapter 739, OAR 125-800-005, 125-800-0010 and 125-800-0020.

### **APPLICABILITY:**

This policy applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 182.122 and 182.124 and OAR 125-800-0020 (3)(a) and (b) and (4) as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

## Statewide Policy

**POLICY NAME:** Information Security

**POLICY NUMBER:** 107-004-052

**ATTACHMENTS:** None.

**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.

**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.

**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.

**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.

**Sensitivity:** A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

**GUIDELINES:** The ISO/IEC 27002:2005 standard identifies controls considered to be common practice for information security as:

- Information security policy document;
- Allocation of information security responsibilities;
- Information security awareness, education, and training;
- Correct processing in applications;
- Technical vulnerability management;
- Business continuity management; and
- Management of information security incidents and improvements.

## Statewide Policy

**POLICY NAME:** Information Security

**POLICY NUMBER:** 107-004-052

Agency information security plans should include the following:

- Administrative safeguards in which the agency:
  - Designates one or more employees to coordinate the security program;
  - Identifies reasonably foreseeable internal and external risks;
  - Assesses the sufficiency of safeguards in place to control the identified risks;
  - Trains and manages employees in the security program practices and procedures;
  - Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
  - Adjusts the security program in light of business changes or new circumstances;
- Technical safeguards in which the agency:
  - Assesses risks in network and software design;
  - Assesses risks in information processing, transmission and storage;
  - Detects, prevents and responds to attacks or system failures; and
  - Regularly tests and monitors the effectiveness of key controls, systems and procedures; and
- Physical safeguards in which the agency:
  - Assesses risks of information storage and disposal;
  - Detects, prevents and responds to intrusions;
  - Protects against unauthorized access to or use of information assets during or after the collection, transportation and destruction of the information; and
  - Disposes of an information asset after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.