DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Policy

SUBJECT:	Employee Security	**NUMBER:**	107-004-053
DIVISION:	Enterprise Information Strategy and Policy	**EFFECTIVE DATE:**	7/30/07

APPROVED: Lindsay A Ball

POLICY/ PURPOSE:

Purpose: The purpose of this policy is to protect information assets and reduce the risk of human error and misuse of enterprise information and equipment.

Policy: Each agency will develop and enforce a policy that:

- Requires pre-employment screen of employees commensurate with the value and risk of the information assets they will have access to;
- Establishes accountability and responsibility to all employees having access to the agency's information assets;
- Establishes processes for timely removal of all permissions for employees having access to information assets and return of agency assets at termination or reassignment; and
- Establishes awareness training for employees.

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 six (6) months 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.

ATTACHMENTS: None.

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 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.

GUIDELINES:

Agency management should ensure that employees and volunteers:

- Are briefed on compliance with agency policies;
- Sign for the receipt of agency policies:
  - Acknowledging receipt of the policies; and
  - Acknowledging their understanding and agreement to comply with agency policies.
- Receive user awareness training;
- Are aware of their roles and responsibilities for the protection of information assets.

Agencies should have documented procedures for the review and classification of appropriate security levels for staff members whose duties have changed due to promotion, demotion, or reassignment.

Voluntary Termination

Agencies should follow normal access control policies and procedures whenever an employee voluntarily leaves state service or accepts a position or job rotation, developmental or work out of classification assignment, within the agency or with another agency. In some cases, agencies may wish to remove access to information assets at the time an employee informs them of his/her intention to leave or accept a job rotation, developmental or work out of classification assignment.

Involuntary Termination

Access to information systems and assets should be removed prior to or at the same time the employee is notified of an involuntary action. Involuntary termination is disciplinary termination or removal from trial service, layoff, or for temporary actions such as duty station at home, suspension with or without pay or administrative leave pending an investigation.