

| | | |
|--|--|-------------------------------------|
| Oregon Public Employees Retirement System | Posted date March 12, 2010 | Number 1.10.01.01.000.POL |
| Signature <i>Paul N. Cleary</i> | Approval date March 10, 2010 | Page 1 of 5 |
| Policy: | Information Security | |
| Objective: | Establishes an information security program that complies with state policies and other federal and state regulations. | |
| References: | DAS Information Security policy (107-004-052) | |

Policy

It is the policy of the state of Oregon to ensure the confidentiality, integrity, and availability of information assets entrusted to the state by its citizens by securing those assets from unauthorized access, modification, destruction, or disclosure and to ensure their physical security.

This policy applies to all employees and individuals working for third parties that have an authorized business relationship with the agency who have been granted access to agency information independent of its form. This policy is modeled after and complies with the DAS Information Security policy (107-004-052).

Management is responsible to ensure all employees and individuals working for third parties understand and adhere to this policy. The security of the agency's information assets is everyone's responsibility. Access to information must be strictly controlled using the least-privilege principle, and information must be used only for business purposes. Executive management is committed to this policy.

PERS will establish an Information Security Program that complies with the DAS security policy framework, state policies, applicable regulations, and relevant industry best practices. The Information Security Program will clearly state organization-wide objectives, identify and assign responsibilities, develop and implement security policies and practices, and provide a framework for monitoring and enforcement.

Information security policies will be reviewed at least annually to accommodate organizational changes and the evolving information security environment.

Roles and responsibilities:

Individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using agency information assets:

Agency Executive Director is responsible for:

Origination date: October 20, 2004

Last revision date: February 23, 2010

Last review date: February 23, 2010

- information assets held by the agency, and
- establishing an information security program that governs:
 - the integrity of information assets,
 - the authorization of access to those assets, and
 - compliance with legal requirements for information confidentiality.

Chief Information Officer (CIO), the Information Services Administrator, is the agency's designated CIO responsible for:

- strategic planning and implementation of information technologies,
- aligning information technologies with statewide technical architecture and standards,
- managing information technology resources, and
- creating and managing a reliable, secure network.

Information Security Officer, the Internal Audits Director, is the agency's designated Information Security Officer responsible for:

- ensuring the development of policies, procedures, baselines, standards, and guidelines by chairing the Information Security Board (ISB);
- establishes and oversees the agency's Information Security Plan;
- convening the Information Security Incident Response Team (InSIRT) when an incident occurs,
- evaluating information security incidents and response;
- communicating with the State Incident Response Team (SIRT) within 24 hours of an incident; and
- coordinating the agency's actions with SIRT in response to an incident that involves information security.

Information Security Board is responsible for:

Origination date: October 20, 2004

Last revision date: February 23, 2010

Last review date: February 23, 2010

SL2

- oversight of the Information Security Program,
- prioritizing information security efforts,
- reviewing and recommending security policies,
- promoting organizational security efforts, and
- recommending strategic direction for information security to the agency director.

Management is responsible for:

- acquiring, developing, and maintaining production applications that process agency information,
- designating data classification levels for systems and data elements,
- defining system service level requirements,
- defining access privileges and approving access requests,
- monitoring compliance,
- investigating information security incidents, and
- establishing procedures to resolve information security policy violations.

Employees, contractors, vendors, and business partners are responsible for:

- complying with all information security policies,
- using information only for agency business purposes, and
- maintaining the confidentiality, integrity, and availability of the information.

Compliance:

All employees, contractors, vendors, and business partners are responsible for understanding and complying with information security policies.

Violation of this policy or associated policies, standards, guidelines, or procedures can result in limitation, suspension, or revocation of system privileges and can lead to other disciplinary action up to

Origination date: October 20, 2004

Last revision date: February 23, 2010

Last review date: February 23, 2010

SL2

and including dismissal for employees or termination of contracts for contractors, vendors, or business partners. Violations can also result in civil and/or criminal prosecution.

Individuals have the responsibility to report suspected policy violations to his or her immediate supervisor, Human Resources, or Internal Audits. All reports of alleged policy violations will be investigated.

Authority: Oregon Revised Statutes and DAS policy

| Number | Policy title |
|--------------|--|
| ORS 646A.600 | Oregon Consumer Identity Theft Protection Act |
| ORS 182.122 | Information Systems Security in Executive Department |
| 107-004-052 | Information Security |

PERS Information Security policies

| Number | Policy title |
|----------------|--|
| 1.10.01.01.008 | Acceptable Use of Information Systems |
| 1.10.01.01.003 | Data Classification |
| 1.10.01.01.001 | Security Breach Response |
| 1.10.01.01.005 | Physical Security - Facility Access Controls |
| 1.01.00.00.017 | Release of Confidential Information |
| 1.01.00.00.028 | Release of Sensitive Information |
| 1.01.00.00.006 | Conflict of Interest and Standards of Conduct |
| 1.01.00.00.033 | Social Security Number Use in PERS-Generated Communications and Correspondence |
| 3.01.01.05.126 | All Systems Access Privileges Cease When Workers Terminate |

Origination date: October 20, 2004

Last revision date: February 23, 2010

Last review date: February 23, 2010

| Number | Policy title |
|----------------|--|
| 3.01.01.08.097 | Limited Number of Privileged User-IDs |
| 3.05.01.00.169 | Compliance with Organizational Systems Development Procedures |
| 3.01.01.03.101 | Approvals Required for User-ID Creation and Privilege Assignment |

Origination date: October 20, 2004

Last revision date: February 23, 2010

Last review date: February 23, 2010

SL2