



Information Security Policy

Subject Information Security	Approval Signature <i>Julie Ruthven</i>
Who this Policy Applies to All agency employees	Approval Date 8/25/2008
Number 20.5.0	Scheduled Review Date

Purpose

Information security policies emphasize the Secretary of State's commitment to information security and provide direction and support for information security in accordance with business requirements and relevant laws and regulations.

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.

- Focused on Security. Dedicated to Success. -

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 to managing risks.

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

Background

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. Oregon Secretary of State is using the ISO 27002 standard to guide the creation of information security policies.

Policy

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.

Creating a Policy Set

The Secretary will implement a set of information security policies that meet the specific operating environment, business requirement and legal needs of the agency.

Review and Evaluation

Agency information security policies and standards will be reviewed on an annual basis to ensure that new business needs and risks, and new or modified business processes are reflected in the information security policies. This review will be conducted by the Oregon Secretary of State Security Officer and the Information Security Review Board and recommended changes will be presented to Management Council for final adoption.

Organizational Responsibilities

The agency security policies will define organizational responsibilities to support information security activities, in conformance with the following requirements:

Organization of Information Security

The agency will establish a framework to initiate and control the

- Focused on Security. Dedicated to Success. -

implementation of information security within the agency. A process must be established to determine information sensitivity, based on best practices, state directives, and legal and regulatory requirements to determine the appropriate levels of protection for that information.

Functional Responsibility

The Information Systems Division Director is responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the Secretary's information assets. The Information Systems Division Director is responsible for ensuring the agency's compliance with state and federal security regulations.

Agency Information Security Officer Function

The Agency must designate a primary contact for information security to act as the security liaison and to guide the agency in compliance to statewide and federal information security regulations. The Agency Information Security Officer (ISO) acts as the security advisor to the agency and is responsible for ensuring that management is aware of current security issues and possible future threats. The ISO also provides recommendation for improvements in information security at the Secretary of State.

Individual Accountability

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

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.

References

- ISO/IEC 27002:2005

- Focused on Security. Dedicated to Success. -