

SUBJECT: INFORMATION SECURITY GOVERNANCE

NOTE:

There is a Collective Bargaining Agreement (CBA) between the State of Washington and the Washington Federation of State Employees (WFSE) that applies to represented employees.

When a topic is covered in the CBA, the policy on that topic applies only to non-represented employees. If the agency's policy conflicts with the CBA, the CBA supersedes the policy for represented employees. Where there is no conflict, the policy supplements the CBA.

PURPOSE:

The purpose of the Information Security Governance Policy is to develop and promote information security policies, standards, and procedures for areas of the enterprise such as privacy, security, project management, application development, wireless, messaging, remote access, outside contractors, and disaster recovery. Additionally, these policies, standards, and procedures will support compliance with Federal Information Security Management Act (FISMA), state, and Employment Security Department (ESD) information security documentation requirements.

Information Security Governance is the responsibility of Employment Security's Senior Leadership Team (SLT). Information Security Governance consists of the leadership, organizational structures and processes that safeguard information. It has a direct relationship to ESD's risk management strategy.

POLICY:

- 1) The Employment Security Department's Senior Leadership Team is responsible for ESD's information security program and ensures compliance with information security policies, standards, and procedures.
- 2) ESD Information Security standards and procedures will be developed, documented, and implemented through the process described in the Information Security Governance Procedure, 4101A.

- 3) The Information Security Manager is assigned responsibility to install, monitor, and manage information security standards and procedures.
- 4) The Information Security Manager is assigned responsibility to develop, implement, maintain, and test information security policies, standards, procedures, and other documents necessary for ESD's information security program.
- 5) The Information Security Manager is assigned responsibility to ensure all agency users of information technology (IT) resources are trained to follow information security policies, standards, and procedures.
- 6) The security verification letter will be submitted to the Office of the Chief Information Officer (OCIO) annually.

DEFINITIONS:

Organizational Governance is a set of responsibilities and practices used by an organization's management to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed, and organizational resources are properly utilized.

Information Technology (IT) Governance is a formalized structure of responsibilities and practices used to direct and control an information technology enterprise toward achievement of its goals. IT governance is an integral part of organizational governance and addresses leadership and organizational structures, practices, and processes necessary to ensure that the IT sustains and extends the organization's strategy and objectives.

Information Security Governance is a component of IT governance, with a specific focus on information integrity, service continuity (availability), and information asset protection (confidentiality).

Policies are high-level management direction endorsed by recognized management authority.

Standards specify the uniform method of support for policy. Compliance with a standard is mandatory. Standards are developed to address existing and newly developed policies using regulatory requirements, best practices and input from areas that are affected.

Procedures are step-by-step instructions to perform desired actions. Procedures provide support for standards. Compliance with approved procedures is mandatory.

FISMA is the Federal Information Security Management Act. FISMA was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include FIPS 199, FIPS 200, and National Institute of Standards and Technology (NIST) Special Publications 800-53, 800-59, and 800-60. Additional security guidance documents were developed in support of the project including NIST Special Publications 800-37, 800-39, and 800-53A.

NIST is the National Institute of Standards and Technology. The NIST Special Publication 800 series was established to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

RELATED DOCUMENTATION:

1. Washington State Office of the Chief Information Officer
<http://ofm.wa.gov/ocio/policies/default.asp>
2. Washington State ISB Policy No. 401-S4:
http://isb.wa.gov/policies/401S_January2008version.doc
3. FISMA Security standards FIPS 199, FIPS 200, and NIST Special Publications 800-53, 800-59, and 800-60: <http://csrc.nist.gov/groups/SMA/fisma/index.html>
4. ESD Policy and Procedure 4000, "Information Security Management"
5. ESD Information Security Governance Standard, 4101
6. ESD Information Security Governance Procedure, 4101A
7. ESD Information Security Governance Exception Procedure, 4101B
8. ESD Policy and Procedure 4200, "Information Security"

SUPERSEDES:

None

DIRECT INQUIRIES TO:

Information Technology Services Division
Brian Barta, [Information Security Manager](#)
(360) 407-4655