Office of the Chief Information Officer (OCIO)	POLICY NO. 141 **Securing Information Technology Assets**
Purpose: Set requirements for maintaining system and network security, data integrity and confidentiality.	**Effective Date:** October 1, 2011 **See Also:** Securing Information Technology Standards (141.10)

POLICY STATEMENT

1. **Agencies will maintain systems, networks, and applications in a manner to ensure:**
    - Availability of information technology (IT) assets.
    - Access to information technology assets is allowed only by authorized individuals.
    - Integrity and privacy of information technology assets is maintained.
    - Misuse or loss of information technology assets is prevented.

2. **Each agency will adhere to this policy and current security standards adopted by the Office of the Chief Information Officer.**

3. **Each agency will operate and maintain information technology assets within an environment that provides a level of security commensurate with:**
    - The sensitivity and importance of each asset's purpose and function.
    - The privacy and confidentiality level of the information content.

4. **Interaction with agency's IT assets will be through an architecture that is compliant with all of the OCIO's policies and standards.**

5. **Each agency will ensure every employee is adequately trained to perform the security procedures for which they are responsible.**

6. **Each agency will establish and maintain an agency security program that includes information technology security policies, procedures, and any other documents necessary to the program.**

    6.1. The agency will review this program at least annually, and make appropriate updates after any significant change to its business operations, computing, or telecommunications environment.

7. **Each agency will conduct an Information Technology Security Policy and Standards Compliance Audit at least once every three years.**

    7.1. The audit will be performed by a qualified party or parties independent of the agency's information technology organization.

7.2. The State Auditor may determine an earlier audit of an agency's information technology security program is warranted.

7.3. The nature and scope of the audit will be commensurate with the extent of the agency's dependence on secure information technology assets to accomplish its critical business functions or as such operations may impact the security of other state agencies.

7.4. The audit will be conducted using audit standards developed and published by the State Auditor.

7.5. Upon completion of the audit, each agency will submit the results of the audit and the plan for correcting material deficiencies to the state Chief Information Officer.

8. Agency heads will provide annual certification to the OCIO that the agency is in compliance with this policy and related standards, and that an Information Technology Security Program has been developed, implemented, and tested.

8.1. The annual security verification letter will be included in the agency information technology portfolio, which is due to the ISB on the same date that the agency's budget submittal is due to the Office of Financial Management.

8.2. The verification letter indicates review and acceptance by the agency head of the agency's security policies, procedures, and any other security program documents, as well as updates to them since the last approval.

9. Entities not governed by this policy that wish to connect to statewide systems governed by this policy must sign a statement certifying that a policy comparable to this policy and related standards are in effect and has been developed, implemented, and tested.

RESPONSIBILITIES

Portions of an agency's IT security program and audit results may contain sensitive or confidential information. Agency policy and procedures for the distribution of this information should consider applicable statutes that exempt specific information from public disclosure and limit distribution to authorized entities and individuals with a legitimate need to know.

Chief Information Officer (or designee)
- Interpret the policy.
- Ensure policy content is kept current.
- Recommend updates to this policy and related resources as needed.
- Develop an escalation process if an agency is not in agreement or compliance.
- Review agency projects for compliance with the security policy.
- Help agencies understand how to comply with the policy.
- Monitor annual compliance by agencies.

Technology Services Board (TSB)
- Review and approve major policy changes.

State Auditor
- Develop, publish, and maintain audit standards for information technology security audits.

Agency Heads
- Ensure and oversee agency's information technology security and compliance with this policy and related standards.
- Ensure agency security policies, procedures and any other documents necessary for the security program are developed, implemented, maintained, and tested.
- Ensure staff is trained to follow security policies, standards, and procedures.
- Submit annual, signed security verification letter.

DEFINITIONS

Information technology assets are the processes, procedures, systems, infrastructure, data, and communications capabilities that allow each agency to manage, store, and share information in pursuit of its business mission, including but not limited to:
- Applications.
- All data typically associated with IT systems regardless of source (agency, partner, customer, citizen, etc.).
- All data typically associated with IT systems regardless of the medium on which it resides (disc, tape, flash drive, cell phone, personal digital assistant, etc.).
- End-user authentication systems.
- Hardware (voice, video, radio transmitters and receivers, mainframes, servers, workstations, personal computers, laptops, and all end point equipment).
- Software (operating systems, applications software, middleware, microcode).
- Infrastructure (networks, connections, pathways, servers, wireless endpoints).
- Services (data processing, telecommunications, office automation, and computerized information systems).
- Telecommunications hardware, software, and networks.
- Radio frequencies.
- Data computing and telecommunications facilities.

Security is defined as the ability to protect:
- The integrity, availability, and confidentiality of information held by an agency.
- Information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction.
- Information technology facilities and off-site data storage.
- Computing, telecommunications, and applications related services.
- Internet-related applications and connectivity.

RELATED LAWS AND OTHER RESOURCES

RCW 42.56.100 - Protection of public records – public access
RCW 42.56.420 - Security
RCW 43.88.160 - Fiscal management. Powers and duties of officers and agencies
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.450 OCS Governance
State Auditor Information on Compliance Audits

Find Your Audit Team

REVISION HISTORY

Date	Action taken
October 2011	Policy reformatted for migration to Office of Chief Information Officer.
January 10, 2008	Added statement #9 requiring comparable security policies for entities wishing to connect to state systems.
November 2006	Revised format; revised Applies To section content; added requirement to submit audit results to the ISB in statement #7; revised annual compliance filing date to match agency's budget submittal date in statement #8; removed language redundant with Information Technology Security Standards, Policy No. 401-S3; simplified and clarified language throughout.
April 2002	Revised format; added language to policy statement #5 on Internet applications; added language to policy statement #8 on agencies providing annual certification to the ISB.
October 6, 2000	Initial effective date.

CONTACT INFORMATION

For questions about this policy, please contact your OCIO Information Technology Consultant.

APPROVING AUTHORITY

Chief Information Officer Date
Chair, Technology Services Board