SEC-03
State CIO Adopted: November 16, 2023
TSB Approved: November 28, 2023
Sunset Review: November 28, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (1.4, 2.1, 4.5)
December 11, 2017

INFORMATION SECURITY AND PRIVACY AWARENESS TRAINING POLICY

See Also:
RCW 43.105.054 WaTech Governance.
RCW 43.105.020 (22) "State agency".
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 52.105.450 (6, 8) Office of Cybersecurity – Higher education, Judicial, and Legislative
Center for Internet Security CIS-18.6

1. **Agencies must ensure all Information Technology (IT) system users are aware of basic information security. See NIST SP 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model.**

    a. Information security training must be completed:

        i. As part of onboarding for new users within 30 days of their start date.

        ii. At least annually.

    b. The security awareness program must minimally include:

        i. A basic understanding of the need for information security.

        ii. User actions to maintain security.

        iii. User actions to respond to suspected security incidents.

2. **Agencies must document and communicate the information security knowledge required for users based on their roles and responsibilities. See NIST SP 800-50 Rev. 1 Building an Information Technology Security Awareness Training Program.**

3. **Agencies must ensure that all users receive sufficient information security and privacy related training to the user's roles and responsibilities and the information systems to which the user has authorized access.**

    a. Agencies must ensure that users receive training that addresses Washington State security policies and standards and the agency's security policies and standards.

b. Agencies will document the frequency of training.

4. **Agencies must retain individual training records according to applicable laws, executive orders, directives, policies, regulations, standards, and guidance, but in no case less than needed to satisfy the requirements of the SEC-09 Audit and Accountability Policy.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. NIST SP 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model.
3. NIST SP 800-50 Rev. 1 Building an Information Technology Security Awareness Training Program.
4. SEC-09 Audit and Accountability Policy.
5. NIST Cybersecurity Framework Mapping:
   - Protect.Awareness Training-1 (PR-AT-1): All users are informed and trained.
   - Protect.Awareness Training-2 (PR-AT-2): Privileged users understand their roles and responsibilities.
   - Protect.Awareness Training-3 (PR-AT-3): Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
   - Protect.Awareness Training-4 (PR-AT-4): Senior executives understand their roles and responsibilities.
   - Protect.Awareness Training-5 (PR-AT-5): Physical and cybersecurity personnel understand their roles and responsibilities.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For questions about Cybersecurity awareness for Washington State employees, please email the Risk Management mailbox.