WaTech
Washington Technology Solutions

IT Security Awareness and Training Policy Background

New, Update or Sunset Review? Sunset Review.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

The original standard items on security awareness were consolidated and modified based on workgroup and community feedback to improve clarity for agency adoption and accountability. The update replaces 141.10 1.4, 2.1,4,5. Additional updates to this policy draw from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Basic cybersecurity awareness training for all IT system users enhances the primary line of defense to maintain business continuity.
- This policy ensures agency staff have awareness and training aligned with their role in IT security.

What are the key objectives of the policy/standard?

- Ensure that users are familiar with potential threats to the IT ecosystem and aware of strategies they must employ to prevent or respond.
- Agency staff who have IT and IT security-related roles are informed and recognize their roles and responsibilities.

How does policy/standard promote or support alignment with strategies?

Strategic Planning | Washington Technology Solutions
This policy supports efficient and accountable government by ensuring agencies are managing IT roles and responsibilities comprehensively.

What are the implementation considerations?

- Agencies will need review and verify that their awareness and training requirements are sufficient
- Agencies may request additional training and support.

- Additional specific training cannot be designated to IT system users who do not already have this included in their job descriptions, but training paths can be suggested.

How will we know if the policy is successful?

Specific: Agency IT system users attest to their awareness of their duties and obligations.
Measurable: Activity and feedback on the awareness and training materials can be reported.
Achievable: WaTech offers basic cybersecurity training awareness for all agencies.
Relevant: People who are unaware of the cybersecurity risk are far more likely to allow a threat into the system than those who receive basic training.
Timely: Ransomware and other malware are easier than ever to deploy, so the risk will only continue to increase.
Equitable: Agencies of all sizes benefit when everyone completes basic cybersecurity awareness training. Agencies with additional resources and responsibilities will have corresponding needs for additional training.

SEC-03
State CIO Adopted:
TSB Approved:
Sunset Review:

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 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) "State agency"
Center for Internet Security CIS-18.6

1. **Agencies must ensure all IT system users are aware of basic information security. See NIST 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 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 800-50 – Building an Information Technology Security Awareness and Training Program.**

3. **Agencies must ensure that all users receive sufficient information security and privacy training related 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 security policies and procedures.

    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 Audit and Accountability Standard.**

REFERENCES

1. NIST 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
2. NIST 800-50 - Building an Information Technology Security Awareness and Training Program
3. Definitions of Terms Used in WaTech Policies and Reports
4. Audit and Accountability Standard

5. NIST Cybersecurity Framework Mapping:
    - Protect.Awareness Training-1: All users are informed and trained.
    - Protect.Awareness Training-2: Privileged users understand their roles and responsibilities.
    - Protect.Awareness Training-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
    - Protect.Awareness Training-4: Senior executives understand their roles and responsibilities.
    - Protect.Awareness Training-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 CAWSE Mailbox.