SEC-04-03-S
State CIO Adopted: August 11, 2023
TSB Approved: September 14, 2023
Sunset Review: September 14, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (5.1.1, 5.6.2)
December 11, 2017

CONFIGURATION MANAGEMENT STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) State Agency
RCW 43.105.205 (3) Higher Ed
SEC-11-01-S Risk Assessment Standard
NIST 800-37r2 Risk Management Framework
NIST 800-128 Guide for Security-Focused Configuration Management

1. **Agencies must create a configuration baseline for all systems that would impact the agency's security posture as part of the agency's security program:**

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems referencing the Center for Internet Security (CIS) benchmarks, and/or vendor-provided secure baseline configuration requirements. See the Asset Management Policy.

      i. If CIS benchmarks and/or vendor-provided secure baseline configuration requirements are not available, the agency must develop, document, and maintain a secure configuration for the solution and may consult with WaTech.

      ii. WaTech will offer additional guidance and services for securing endpoints using CIS benchmarks. Agencies must utilize the Endpoint Detection Response (EDR) solution where applicable.

   b. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system baseline configurations. Identify, document, and approve any deviations from established configuration. See Securing IT Assets Section 6.1, 6.2 Access Control.

   c. Retain one previous version of baseline configurations of information systems to support rollback.

   d. Monitor and control changes to the configuration settings in accordance with the Change Management Policy.

   e. Review and update the baseline configurations annually or after changes to that baseline.

2. **Agencies must exercise configuration change control for all systems that would impact the agency's security posture:**

   a. Determine the types of changes to the information system that affect its configuration and their potential impacts. Configuration change control documentation must be handled, at minimum, as category 3 information.

   b. Test, validate, and document the proposed information system configuration change prior to implementation. This must include identification of potential security impacts.

c. Document configuration change decisions associated with the information system.

d. Implement approved configuration changes to the information system.

e. Retain records of configuration changes for the period of one year after the date of the change according to the required retention period. See GS 14020 Rev. 1 State Government General Records Retention Schedule v.6.1.

f. Perform an annual internal review of configuration changes to ensure compliance with internal change management processes.

3. **Agencies must configure all information systems that would impact the agency's security posture to provide only business-related capabilities and prohibit the use of functions, ports, protocols, and/or services that are not required for business functions.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports.
2. CIS Benchmarks.
3. SEC-04 Asset Management Policy.
4. SEC-05 Change Management Policy.
5. Securing Information Technology Assets Standards (Parts Rescinded) 141.10 (2) - Access Control Policy.
6. GS 14020 Rev. 1 State Government General Records Retention Schedule v.6.1.
7. NIST Cybersecurity Framework Mapping:
    - Detect.Anomalies and Events (DE.AE-1): A baseline of network operations and expected data flows for users and systems is established and managed.
    - Protect.Information Protection Processes and Procedures (PR.IP-1): A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
    - Protect.Information Protection Processes and Procedures (PR.IP-2): A System Development Life Cycle to manage systems is implemented.
    - Protect.Protective Technology (PR.PT-3): The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For a Security Design Review or for technical security questions, please email the Security Design Review Mailbox.
- For questions about risk assessments and management, please email the Risk Management Mailbox.