SEC-04
State CIO Adopted: June 8, 2023
TSB Approved: June 8, 2023
Sunset Review: June 8, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (8.2)
December 11, 2017

ASSET MANAGEMENT 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
OFM 30.45.10 Physical inventory frequency
MGMT-03 Business Application/System Governance
MGMT-01-01-S Technology Portfolio Foundation
SEC-04-03-S Configuration Management Policy
SEC-02-01-S Application Security Standard (Pending Policy – See 141.10 7)

1. **Agencies must establish and maintain an inventory of IT infrastructure. See NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.**

    a. Hardware inventory must include, if applicable, the inventory attributes specified in MGMT-01-02-S Technology Portfolio Foundation - Infrastructure.

    b. This includes those managed by the agency, a third-party agency, or a third-party vendor, and a description of who is managing the infrastructure.

    c. Inventory information must be handled, at a minimum, as category 3 information, according to SEC-08-01-S Data Classification Standard.

    d. Agencies must review and update the infrastructure inventory annually.

    e. For systems that process category 3 or category 4 data:

        i. Update the inventory of system components as an integral part of component installations, removals, and system updates.

        ii. Employ tools that detect, alert, and report the presence of unauthorized hardware, software, and firmware components within the system on a quarterly frequency.

        iii. When detected, remove or quarantine unauthorized components from the network.

2. **Agencies must establish and maintain an inventory of all applications.**

    a. This includes applications installed on servers and workstations, as well as Software as a Service (SaaS) solutions.

    b. Inventory information must be handled, at a minimum, as category 3 information.

    c. Agencies must review the application inventory annually to ensure that only currently supported applications are authorized.

    d. Application inventory must include the inventory attributes specified in MGMT-01-01-S Technology Portfolio Foundation - Applications Standard.

3. **Agencies must also update the asset inventory when:**

    a. Moving or transferring an asset outside agency control.

b. An asset is lost, stolen, nonrepairable or obsolete.

c. An asset is no longer needed or needs to be repurposed/disposed.

4. **Agencies must satisfy the requirements established in the SEC-04-02-S Media Sanitization and Disposal Standard when planning asset transfer or disposal.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports
2. NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations
3. MGMT-01-02-S Technology Portfolio Foundation - Infrastructure
4. SEC-08-01-S Data Classification Standard
5. MGMT-01-01-S Technology Portfolio Foundation - Applications
6. SEC-04-02-S Media Sanitization and Disposal Standard
7. NIST Cybersecurity Framework Mapping:
   - Identify.Asset Management-1 (ID.AM-1): Physical devices and systems within the organization are inventoried.
   - Identify.Asset Management-2 (ID.AM-2): Software platforms and applications within the organization are inventoried.
   - Protect.Data Security-8 (PR.DS-8): Integrity checking mechanisms are used to verify hardware integrity.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- To request a Security Design Review or for technical security questions, please email the Security Design Review Mailbox.