Policy & Standard Background

Name: Asset Management Policy

Replaces IT Security Standard 141.10 (8.2)

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.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this standard draws from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- A centralized inventory of hardware and software assets enables agencies to make sound business, technical, and legal decisions.
- This standard helps agencies ensure only appropriate hardware are connected to the agency's network to allow for quick recognition of unauthorized devices.

What are the key objectives of the policy/standard?

The objectives of this standard are:

- Ensuring agencies have a clear picture of the agency's infrastructure and software profile.
- Inventory data is handled at an appropriate classification level.

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

Strategic Planning | Washington Technology Solutions

This standard supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

What are the implementation considerations?

- Agencies will need resources to review and verify current inventories.
- Agencies may need additional training and support.

How will we know if the policy is successful?

- Agencies will use centralized inventories to understand the agency's IT profile and support a secure environment.
- Agencies maintain their inventory when changes happen.

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

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

ASSET MANAGEMENT POLICY

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
RCW 43.105.450 (7c) IT Security
OFM 30.45.10 Physical inventory frequency
IT Policy 114 Business Application/ System Governance

1. **Agencies must establish and maintain an inventory of IT infrastructure**.

    a. Hardware inventory must include, if applicable, the inventory attributes specified in Standard 112.20 – Infrastructure Items.

    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 the 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 Standard 112.10 – Application Items.

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 Media Sanitization and Disposal Standard when planning asset transfer or disposal.**

REFERENCES

1. Application Security Standard (Pending Policy – See 141.10 7)
2. Data Classification Standard
3. Configuration Management Policy (Pending Policy – See 141.10 5.1.1)
4. Media Sanitization and Disposal Standard (Pending Policy - See 141.10 8.3)
5. Definitions of Terms Used in WaTech Policies and Reports
6. Policy 112 – Technology Portfolio Foundation
7. Standard 112.10 – Technology Portfolio Foundation - Application Items
8. Standard 112.20 – Technology Portfolio Foundation - Infrastructure Items
9. NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
10. 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.