WEBER STATE UNIVERSITY
Information Technology

Inventory and Control of Enterprise Assets Standard (CIS CSC 1)

Introduction

This standard intends to reach compliance with CIS Control 1. Enterprise asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by an enterprise. Enterprise asset management is a complex challenge for an enterprise of any size. New assets are constantly acquired, others are retired, and many are lost. With work from home becoming more prominent, enterprise assets may disappear from the primary enterprise network, only to reappear months later or never again. Multiple types of enterprise assets often need to be managed differently. Enterprises may perform asset management manually, employ a database or spreadsheet, or use dedicated asset management software.

Scope

This standard applies to all enterprise assets that have the potential to store, process, or transmit data within the organization. This standard is designed to guide the management of these assets throughout their lifecycle, from acquisition to disposal, ensuring they are tracked, maintained, and secured in compliance with CIS Controls v8 standards.

Purpose

The Inventory and Control of Enterprise Assets standard aims to establish a robust framework for identifying, managing, and securing all hardware assets within Weber State University's (WSU) network. This control emphasizes the critical need for WSU to maintain a comprehensive and up-to-date inventory of all assets capable of processing or storing information. The objective is to ensure that only authorized devices can access the network, reducing the risk of unauthorized access and potential cybersecurity threats.

Critical aspects include the creation of a detailed asset inventory that documents all network-connected devices, along with their ownership, classification, and security configuration status. This inventory is a foundational element for effective cybersecurity management, enabling WSU to apply security policies consistently, manage risks more effectively, and respond more quickly to incidents. By implementing the Inventory and Control of Enterprise Assets standard, WSU can achieve higher visibility over digital assets, laying the groundwork for a secure and resilient IT environment. This standard applies to all departments, colleges, and all assets connected to the WSU network. WSU will strive for IG2 compliance in accordance with §16 CFR 314.4(d) and USHE Policy R345.

Responsibility

Departments that acquire IT assets are responsible for ensuring they comply with the configuration requirements defined in this standard. Departments may delegate the responsibility of configuring those assets to one or more local IT administrators, who are held accountable for properly configuring those assets.

Enterprise Asset Lifecycle

Identifying and tracking enterprise assets is essential in the *Enterprise Asset Lifecycle*. An enterprise must first know what is on the network to protect a network. In addition, many other security controls depend on the enterprise asset inventory, such as data management, secure configuration of assets, access control, and more. *Figure 2* shows the high-level "steps" of the *Enterprise Asset Lifecycle*, followed by a detailed description of what each step entails.

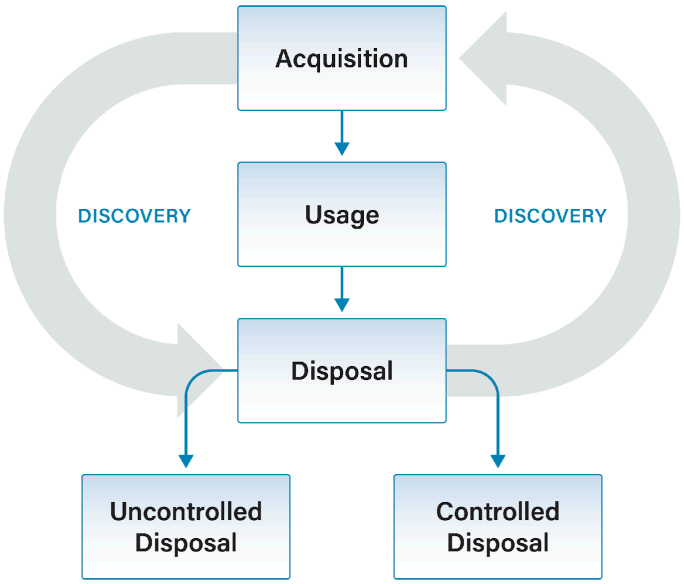

Figure 2. Enterprise Asset Lifecycle

- **Acquisition** – Purchasing new enterprise assets or obtaining new enterprise assets by transfer from another business unit.
- **Discovery** – Identifying new enterprise assets by actively searching for systems connected to the enterprise network. This process is constantly occurring throughout the lifecycle of an enterprise asset.
- **Usage** – The authorized use of enterprise assets by users. For this standard, users may include employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user who operates an enterprise asset.
- **Controlled Disposal** – Retiring enterprise assets in a secure manner.
- **Uncontrolled Disposal** – Lost, stolen, or otherwise unaccounted-for enterprise assets.

Acquisition

The acquisition process generally consists of purchasing new enterprise assets from external vendors, including from managed service providers (MSPs) and cloud service providers (CSPs), or obtaining new enterprise assets by transfer from another business unit within the same enterprise. All hardware procurement must abide by WSU PPM 5-25 (5-25 University Procurement/Table of Contents (weber.edu)) as well as Utah State procurement code.

See the Computing Documentation Standard providing guidance for documenting and managing all University computing equipment addressed in PPM 10-1, Information Security Policy. See PPM 5-27, Surplus Property and PPM 5-28, Fixed Asset Accounting.

Discovery

The IT Division will be leveraging security tools in the future as determined.

Usage

A set of rules governing how a user can leverage enterprise assets to perform their job should be in place and adequately communicated to the user. Users must accept and comply with WSUs PPM 10-2, Acceptable Use Policy.

Uncontrolled Disposal

Users will lose or relinquish their enterprise assets from time to time. Uncontrolled disposal of enterprise assets includes a user losing their device or having it stolen. It is often difficult to tell precisely what occurred. In either scenario, enterprise access from that asset must be removed as soon as possible, and the data may need to be wiped from the asset. Users need to be trained to report this occurrence immediately so that IT can act quickly. A report should be filed with law enforcement, often required for insurance and liability reasons. The enterprise asset should be noted as stolen or lost in the asset inventory.

Controlled Disposal

See PPM 5-27, Surplus Property and PPM 5-28, Fixed Asset Accounting. See Computing Documentation Standard and R572, Noncapital Asset Inventory and Tracking where applicable.

This phase of the lifecycle will be how enterprise assets reach their end of life. Assets to be decommissioned must be returned from users *to their designated IT contact* so that user data can be retrieved and/or transferred as necessary. Then, all enterprise data can be securely removed from the enterprise asset as required in the *Data Management Plan*. The device should be noted as retired or decommissioned in the enterprise asset inventory. Access to enterprise data should be revoked for this device.

Acquisition - *Implementation Group 2: Safeguard 1.1 & 1.4*

1. The IT asset owner shall assign unique identifiers to all existing and newly acquired enterprise assets.
2. Where applicable, each enterprise asset (e.g., desktops, laptops, servers, tablets), must have an enterprise asset tag affixed to the device with this identifier.
3. Automated Inventory Tools: Utilize automated inventory management tools to register new assets as soon as they are acquired. These tools should be capable of scanning and recognizing new devices and adding them to the centralized asset inventory. Configure the active discovery tool to execute daily, or more frequently.
4. Maintain a CMDB: Integrate discovery tools with a Configuration Management Database (CMDB) or a similar centralized repository where detailed information about each asset, including its configuration, current status, and history of changes, is maintained. This integration helps maintain a dynamic and accurate inventory of assets.
5. Record the enterprise asset identifier alongside other relevant information within the IT inventory. This is to include:
    a. Enterprise asset identifier
    b. Date of purchase
    c. Purchase price
    d. Item description
    e. Manufacturer
    f. Model number
    g. Serial number
    h. Name of the enterprise asset owner (e.g., administrator, user), role, or business unit, where applicable.

i. Physical location of enterprise asset, where applicable

j. Physical addresses (Media Access Control (MAC))

k. Warranty expiration date

l. Any relevant licensing information

6. Security Configuration and Baseline:

   a. Initial Security Configuration: Configure new assets to comply with organizational security policies before deployment. This includes installing necessary security software, applying patches, and setting secure configurations.

   b. Baseline Configuration: Establish a baseline configuration for different types of assets to ensure consistency and ease of management. Baselines should be regularly reviewed and updated based on evolving security requirements.

7. Access Control and Network Integration:

   a. Access Control Policies: Implement access control policies to define which assets are allowed to connect to the network. This includes authentication and authorization measures to verify the legitimacy of devices.

   b. Network Segmentation: Consider using network segmentation to limit access and reduce potential attack surfaces. Newly acquired assets should be placed in appropriate segments based on their function and security level.

8. Enterprise asset owners must verify the enterprise asset inventory data annually or more frequently once the CMDB is implemented.

Discovery - *Implementation Group 2: Safeguard 1.2 & 1.3*

1. Enterprise assets not included within the inventory must be investigated, as these assets may be unauthorized.

   a. Unauthorized assets not owned by the enterprise must be removed from the network unless the IT division grants temporary access.

   b. Assets owned by the enterprise but not kept within the enterprise asset inventory must be added to the inventory.

2. Users are required to connect their enterprise assets to the enterprise network on a weekly basis, where practical.

3. The IT division must remove the unauthorized asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

4. Network Access Control (NAC)

   a. Implement Network Access Control: Use NAC solutions to automatically detect and prevent unauthorized devices from accessing the network. NAC systems can enforce compliance with security policies before allowing devices to connect, enhancing the network’s security.

5. Cloud and Virtualized Asset Discovery

   a. Discover Cloud and Virtual Assets: Ensure the discovery process includes assets hosted in cloud environments and virtualized assets. This often requires integrating with cloud service providers' APIs or using tools to scan virtual environments to identify and inventory virtual machines and containers.

6. Unauthorized Device Detection

   a. Detect Unauthorized Devices: Implement mechanisms to detect and alert ~~on~~ the presence of unauthorized devices. This may involve anomaly detection techniques or comparing detected devices against the authorized inventory to identify discrepancies.

7. Secure Configuration Verification
    a. Verify Secure Configurations: As part of the discovery process, verify that newly discovered assets are configured securely according to the organization's baseline security configurations. This might involve automated scanning for deviations from the secure baseline.
8. Documentation and Reporting
    a. Maintain Documentation: Keep detailed documentation of the discovery processes, including methodologies, tools used, and integration points. Regularly report on the status of the asset inventory, including insights on compliance with security policies and identification of unauthorized devices.

Usage

1. All WSU enterprise asset users must comply with PPM 10-2, Acceptable Use Policy of University Information Technology Resources
2. Bi-annual, or more frequent, verification of each enterprise asset must be completed in-person or remotely unless an exemption is authorized by supervisory management.
3. It is also the responsibility of the enterprise asset owner to:
    a. Maintain control over the enterprise asset.
    b. Contact IT with any problems such as malfunctions, needed repairs, and underutilized equipment or in the event of equipment loss.
4. IT Access Control Measures
    a. Implement Least Privilege Access: Ensure users have only the access levels necessary for their roles, minimizing potential damage from insider threats or compromised accounts.
    b. Utilize Multi-Factor Authentication (MFA): Deploy MFA for accessing sensitive systems and data, significantly reducing the risk of unauthorized access through compromised credentials.
5. Monitor and Manage Asset Usage
    a. Continuous Monitoring: Employ tools for continuously monitoring hardware asset usage to detect unauthorized activities or non-compliance with usage policies. This includes monitoring ~~for~~ the use of unauthorized applications and data transfer activities.
    b. Log Management: Collect, manage, and analyze logs from hardware assets to track access and activities, supporting incident detection and forensic analysis.
6. Implement Endpoint Protection Solutions
    a. Deploy Endpoint Security: Use comprehensive endpoint security solutions that include antivirus, anti-malware, intrusion detection/prevention, and firewall capabilities to protect hardware assets from threats.
7. Software and Application Control
    a. Control Software Installation and Execution: Implement application whitelisting or allowlisting to control which software can be installed and executed on hardware assets. This helps prevent the execution of malicious or unauthorized software.
8. Data Encryption
    a. Encrypt Sensitive Data: Ensure that sensitive data stored on or transmitted by hardware assets is encrypted, protecting it in case of interception or unauthorized access.
9. Usage Policy Enforcement:
    a. Regularly review and enforce compliance with hardware asset usage policies. Implement disciplinary measures for non-compliance and continuously update policies to address new threats and technologies.

Controlled Disposal

1. Enterprise assets to be decommissioned or retired must be returned to the IT asset owner (PPM 5-27, Surplus Property).
2. The IT division must make a copy of the user data as needed.
3. IT will be responsible for the secure erasure of the primary memory storage device within the enterprise asset, where applicable.
    a. Data Wiping: Implement procedures for securely wiping data from hardware assets before disposal. This may involve using software tools that overwrite data multiple times to prevent data recovery.
    b. Physical Destruction: For highly sensitive data or when data wiping is insufficient, consider physical destruction methods, such as shredding or degaussing, to ensure data cannot be recovered.
4. Enterprise asset owners will be responsible for updating the status or removal of the enterprise asset within all enterprise management systems.
    a. Enterprise asset owners must ensure that records are retained in the asset management system.

Retention of Records

The university follows the retention schedule approved by the State Records Committee. The university follows the Utah General Retention Schedule to retain any record not found under the university's approved retention schedule.

5. Document the removal of the enterprise asset from the enterprise within the asset inventory.
6. Certification of Disposal
    a. Disposal Documentation: Maintain documentation of the disposal process for each asset, including methods of data sanitization used and final disposition of the asset. This documentation serves as evidence of compliance with disposal policies and regulatory requirements.
7. Vendor Management for Disposal
    a. Vendor Selection: If using third-party vendors for asset disposal, select vendors that comply with industry standards for secure disposal and data destruction.
    b. Vendor Oversight: Monitor vendor compliance with contractual obligations related to secure disposal, including conducting audits or requiring certificates of destruction to verify that assets are disposed of securely.
8. Training and Awareness
    a. Educate Staff: Train relevant staff on the procedures and importance of secure asset disposal. This includes educating employees about handling decommissioned assets and the potential risks of improper disposal.
9. Review and Update Disposal Processes
    a. Continuous Improvement: Regularly review and update disposal policies and procedures to address new challenges, technologies, and regulatory requirements. This ensures that disposal practices remain effective and compliant over time.

Uncontrolled Disposal

1. All lost or stolen enterprise assets must be immediately reported to the appropriate business units, including IT, cybersecurity, and finance.
2. A report must be filed with law enforcement for all enterprise assets assumed stolen.

3. Lost and stolen enterprise assets must have their access to enterprise data revoked as soon as possible.
    a. The enterprise assets must also be removed from the inventory.

Note: The following appendices correspond to each CIS CSC Standard:
Appendix A
Appendix B

Revision History
Creation Date: August 30, 2024
Amended: N/A