

Enterprise Asset Management

Purpose

Enterprise asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by an enterprise. The *Enterprise Asset Management* standard provides the processes and procedures for governing the enterprise asset lifecycle while an enterprise is using an asset. An inventory must be created and maintained to support the enterprise's mission. This inventory must be current and reflect the current assets owned and operated by the enterprise.

Responsibility

The IT business unit is responsible for all enterprise asset management functions. This information is relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any enterprise assets assigned to them.

Policy

Acquisition

Implementation Group 1: Safeguard 1.1

1. The IT business unit shall assign unique identifiers to all existing and newly acquired enterprise assets.
2. Each enterprise asset (e.g., desktops, laptops, servers, tablets), where applicable, must have an enterprise asset tag affixed to the device with this identifier.
3. 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 (Media Access Control (MAC)) address
 - k. Internet Protocol (IP) address
 - l. Warranty expiration date
 - m. Any relevant licensing information
4. IT must verify the enterprise asset inventory every six months or more frequently.

Discovery

Implementation Group 1: Safeguard 1.2

1. Enterprise assets not included within the inventory must be investigated, as these assets may be unauthorized.
 - a. Assets not owned by the enterprise must be removed from the network unless temporary access is granted by the IT business unit.
 - 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. Permanently air-gapped systems must be approved by IT.
4. IT must address unauthorized assets on a weekly basis at a minimum.
5. IT must choose to remove the unauthorized asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Usage

In general, refer to the enterprise's *Acceptable Use Policy*. The following can substitute until an appropriate policy is created:

1. Users must handle all enterprise assets with care.
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 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.

Controlled Disposal

1. Enterprise assets to be decommissioned or retired must be returned to IT.
2. IT 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.
4. IT will be responsible for updating the status of the enterprise asset within all enterprise management systems.
 - a. IT must ensure that records are retained in compliance with the *Record Retention Policy*.
5. Document the removal of the enterprise asset from the enterprise within the asset inventory.

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.

Revision History

Version	Revision Date	Revision Description	Name
v1.0	01/02/2023	Initial Written Standard	Scott Tisinger