Policy number	Title:	Effective Date:
<your ID format>	HARDWARE ASSET MANAGEMENT POLICY	<your date format>

REFERENCE

- CIS Control 1, IG1 – Inventory and Control of Enterprise Assets, NIST CSF ID.AM-1

SUPPORTING DOCUMENTS

- **<This is a contents link space for any related documentation>**

CONTENTS

PURPOSE

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

SCOPE

The IT business unit is responsible for all 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 assets assigned to them.

It is important to note that this Hardware Asset Management Policy **does not** include assets that do not store, process, or transmit data, such as monitors and keyboards.

POLICY

<company name> is required to maintain an asset inventory list of hardware assets, including all system components (e.g., network address, machine name and OS version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

ASSET DEFINITIONS

Assets are defined as all end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers that exist in virtual, cloud-based, or physical environments, including those that can be connected to remotely. Assets are managed by the enterprise and have the potential to store, process, or transmit data.

Types of assets include:

- End-user devices, such as desktops, workstations, laptops, tablets, and smartphones
- Network devices, such as wireless access points, switches, firewalls, physical/virtual gateways, and routers
- Non-computing/Internet of Things (IoT) devices, such as Industrial Control Systems (ICS), smart screens, printers, physical security sensors, and IT security sensors
- Servers, such as web servers, email servers, application servers, and file servers

NEW ASSET ACQUISITION

1. **<company name>** IT must record a new hardware asset alongside other relevant information within an IT asset inventory list.

   This list is to include:

   - Name of the asset owner or dept (required)
   - Physical location of asset, where applicable (required)
   - MAC address (required)
   - IP address (required)
   - Hostname (required)
   - Manufacturer (if possible)
   - Model number (if possible)
   - Serial number (if possible)

2. IT must verify the hardware asset inventory list every month or more frequently.

ASSET DISCOVERY

All assets must be investigated and unauthorised assets identified.

- Assets not owned by the enterprise and considered unauthorized, must be removed from the network unless temporary access is granted by the IT business unit.
- Assets owned by the enterprise, but not kept within the asset inventory list, must be added to the inventory list.
- Users are required to connect their assets to the enterprise network on a weekly basis at a minimum, where practical.
- Permanently air-gapped systems must be approved by IT.
- IT must address unauthorized assets on a weekly basis at a minimum.
- 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 AND RESPONSIBILITY FOR IT EQUIPMENT

Refer to the **<Acceptable Use Policy>** on usage and responsibility.

CONTROLLED DISPOSAL

This phase of the lifecycle will be how assets reach their end of life. Assets to be decommissioned need to be returned from users to IT so that user data can be retrieved and/or transferred as necessary. Then all enterprise data can be removed from the asset in a secure fashion in accordance with the **<Data Management Policy>**. Assets may then be sold to third-party providers for resale or securely destroyed. The device should be noted as retired or decommissioned in the asset inventory and access to enterprise data should be revoked for this device.

Refer to the **<Asset Secure Disposal Plan>**

UNCONTROLLED DISPOSAL

Users will lose or relinquish their assets from time to time. Uncontrolled disposal of assets includes a user losing their device or having it stolen. It is often difficult to tell exactly what occurred. In either scenario, enterprise access from that asset needs to 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 right away so that IT can act quickly. A report should be filed with law enforcement, which is also often required for insurance and liability reasons. The asset should be noted as stolen or lost in the asset inventory.

- All lost or stolen assets must be immediately reported to the appropriate business units, including IT, cybersecurity, and finance.
- A report must be filed with law enforcement for all assets assumed stolen for insurance purposes.
- Lost and stolen assets must have their access to enterprise data revoked as soon as possible.
    - The assets must also be removed from the asset list.

COMPLIANCE

Create a company specific set of compliance rules. Eg:

In the event of failure to comply with any IT Policy, **<company name>** may at its sole discretion:

- Restrict or terminate a user's right and ability to use or access any or all **<company name>**'s IT systems and facilities.
- Withdraw or delete any data that contravenes this policy.
- Any disciplinary action arising from a breach of this policy shall be dealt with in accordance with the **<company name>** Disciplinary Policy.