Asset Management Policy

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

A. ASSET TYPES

The following minimal asset classes are subject to tracking and asset tagging:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Printers, copiers, fax machines, and multifunction print devices
- Handheld devices
- Scanners
- Servers
- Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
- Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components
- Capital assets purchased with Federal Funds

B. ASSET TRACKING REQUIREMENTS

The following procedures and protocols apply to asset management activities:

- All assets must have an internal asset number assigned and mapped to the device's serial number.
- An asset-tracking database shall be created to track assets. It shall minimally include purchase and device information including:
    - Date of purchase
    - Make, model, and descriptor
    - Serial Number
    - Location
    - Type of asset

- Owner
- Department
- Purchase Order number
- Disposition

Prior to deployment, staff shall assign an ID to the asset and enter its information in the asset tracking database. All assets maintained in the asset tracking database inventory shall have an assigned owner.

C. ASSET DISPOSAL AND REPURPOSING

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

When disposing of any asset, sensitive data must be removed prior to disposal. IT staff shall determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using low level formatting and degaussing techniques. For media storing confidential or student personally identifiable information that is not being repurposed, disks shall be physically destroyed prior to disposal.