IT Asset Inventory Standard

Standard

The University of Cincinnati must maintain an accurate, detailed, and up-to-date inventory of all enterprise computing assets. This inventory includes university owned end-user devices, networking devices and servers. The inventory needs to be detailed enough to support the needs of the various departments within the university community.

The purpose of this standard is to establish the required data elements to be recorded and tracked during inventory of information technology (IT) assets and when these data elements are to be updated.

Inventory of IT System Assets

The Dean or Department Head of each group is responsible for administering these guidelines within their unit or department.

- University-owned technology assets (see definition below) should have an Asset Tag
- Asset tags should be attached, recorded, and tracked by the appropriate IT support organization
- Computer names, also known as “Hostnames”, must be unique for each asset
- Hostnames should start with the generally accepted abbreviation of the department to which the asset is assigned, (ex. DTS, COM, CECH), with the remaining characters left up to the discretion of the individual department or unit based upon their documented standards.
    - Because hostnames are discoverable, and therefore not private, no personally identifiable, university restricted, or potentially sensitive information should be included in the hostname
- University-owned technology assets must be assigned to a department or unit for management and an individual with employee affiliation with the university

System Inventory records must include the following details:

Asset Tag	Capital asset tag for assets over $5,000 Inventory asset tag for all other IT assets
Asset Type	Server, workstation, laptop, printer, network appliance, etc.
System Name	Computer name, hostname, or DNS name
Manufacturer, Make, Model	Ex. Dell PowerEdge R720
Serial number	Manufacturer assigned serial number
Operating system name, and version	Ex. Windows 11, 22H2
Local IP address	10.X.X.X address for devices with static IPs
External IP address	129.137.X.X address for Internet-facing assets
Physical Location	Building, room, and rack location if applicable. Devices assigned to employees working remotely should be marked so. Hypervisor information can be noted here.
Responsible Department	Department with financial responsibility for the asset
Assignment	User to whom the access is currently allocated
Status	In stock, deployed, awaiting disposal, etc. See table below
Department Responsible for Hardware Maintenance	Department with hardware maintenance and asset tracking responsibility for the asset
Department Responsible for Operating System Maintenance	Department responsible for maintaining the operating system and OS vulnerability remediation
Department Responsible for the Application Maintenance	Department responsible for maintaining the application or customer-facing service and application vulnerability remediation
System Criticality	Rating of the criticality of the asset to university operations – High, Medium, or Low
Business Case	Additional information on the asset that supports life cycling, incident response, SLAs, etc. Ex. SQL server supporting DBs for Bearcat Card
Cost Center	Finance cost center under which the asset was purchased or currently resides if transferred

IT Asset Criticality Assessment and Documentation

Criticality is a risk assessment process. The overall risk is determined by the likelihood of failure and the impact of failure. The assets that have the greatest probability of failure and the greatest consequences due to failure will be the assets that are the highest risk and therefore the most critical. The assets that have low likelihood of failure and low consequences if there is a failure will be the least critical assets. The university rates system criticality as Low, Moderate or High.

To determine the Impact on the university there are several factors to consider. The chart below can assist an asset owner in determining the potential impact on the university.

Asset Characteristics	**Impact Characteristics**		
	Low	**Moderate**	**High**
Data	System processes and/or stores public data	System processes and/or stores non-public or controlled data	Systems processes and/or stores restricted data
Community	System affects a single or small group of users	System affects one or more departments or colleges	System affects most of university community
Service	System provides an informational or non-critical service	System provides a moderately important service	Systems provides a critical service

Asset Inventory Updates

The IT Asset inventory must be updated annually and when:

- Purchasing an IT asset
- Moving or transferring an IT asset
- Assigning or loaning an IT asset
- Returning IT asset to inventory from assignment or maintenance
- Sending an IT asset for repair or maintenance
- An IT asset is lost, stolen, nonrepairable or obsolete
- An IT asset is no longer needed and needs to be repurposed/disposed
- An IT asset is sent to surplus

The chart below can assist an asset owner in determining the asset status.

Status	Explanation
In Stock	Tagged, imaged, stored ready for deployment
Reserved	Allocated to specific user, not deployed
Deployed	Equipment delivered to user
Bench	Arrived, tagged, ready to image, recovered equipment waiting for reimage
On Loan	Equipment loaned to a user on a temporary basis
Out of Service	Equipment is damaged, in need of repair, sent for repair to 3rd party
Awaiting Disposal	Equipment is waiting to be disposed
Disposed	Equipment has been removed from site, a certification of destruction and transfer received
In Transit	Moving inventory to new location for build and deployment

For any university asset that is lost or stolen and immediate report to the Office of Information Security and a completed UCPD report are required.

Definitions

Technology Assets - Assets owned by the University of Cincinnati that consist of the following equipment types:

- Servers
- Storage arrays
- Desktop Computers
- Laptop Computers
- Tablets and phones
- Network equipment
- Printers
- Monitors
- Vendor-specific technology appliances
- Projectors and AV equipment

Related Links

Data Governance and Classification Policy

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu