



SPACE INSTITUTE

UT Space Institute IT Procedure: Asset Management	
Version: 1	Effective Date: 10/01/2025

Purpose

To provide guidance and structure for the campus to create and maintain consistent processes for procuring, identifying, tracking, maintaining, and disposing of Information Technology assets.

Scope

This procedure applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

This procedure applies to University owned or managed Assets, Systems, and Resources only. It does not apply to Assets, Systems, and Resources not owned by the University unless specifically stated in the policy.

Procedure

I. University Hardware Asset Management Procedure

University hardware assets are to be procured by the Computer Services department through approved marketplace vendors only. After purchase, university-owned hardware assets must be assigned a unique identifying number displayed on a physical tag on the machine. A UTSI helpdesk ticket is to be generated with the following information to be stored in the centralized inventory database.

- i. University Asset identifier
- ii. Date of purchase
- iii. Item description
- iv. Manufacturer
- v. Model number
- vi. Serial number
- vii. Name of the University Asset Custodian role (e.g., administrator, user), and business unit, where applicable.
- viii. Physical location of University Asset, where applicable
- ix. Physical (Media Access Control (MAC)) address

UT Space Institute IT Procedure: Asset Management	
Version: 1	Effective Date: 10/01/2025

To ensure timely and efficient patch and antivirus management, University hardware assets that are connected to the network must be added to the Active Directory domain using the service tag/serial number as the device name.

Network access is granted via CS approval by patching in to network switches across campus. All switches are secured in locking racks or closet areas with restricted access to ensure users cannot plug unauthorized devices into the network. Inventory, domain membership, and network switch port access is reviewed in-person annually. Unauthorized devices are removed from the domain with MAC address blocked in DHCP to prevent further access.

Assets that are to be decommissioned or retired must have their primary memory storage erased and destroyed. CS Technicians will create a UTSI helpdesk ticket documenting the unique UT tag of the asset and the serial number of the storage device before physically destroying the device. An update to the centralized inventory will be made noting that the device has been removed from use.

All lost or stolen assets must be immediately reported to the UTSI helpdesk. All assets assumed stole will be reported to law enforcement. Local and remote access available to and from these devices must also be removed immediately.

II. University Software Asset Management Procedure

University software assets are to be procured by the Computer Services department through approved vendors only. Any software installed on University hardware assets will be inventoried in a centralized inventory database that contains the following information.

- i. Title of software
- ii. Developer or publisher of software
- iii. Version
- iv. Date of acquisition
- v. Business purpose
- vi. Uniform Resource Locator (URL)
- vii. End-of-support (EoS) date, if known
- viii. End-of-life (EOL) date, if known
- ix. Any relevant licensing information
- x. Decommission date



SPACE INSTITUTE

UT Space Institute IT Procedure: Asset Management	
Version: 1	Effective Date: 10/01/2025

xi. Software Asset Custodian

To request the acquisition or installation of software, users must enter a UTSI helpdesk ticket. Software will then be installed by the CS technician or the users' privileges temporarily escalated to allow the install.

Software inventory will be reviewed and verified using automated tools (currently SCCM) monthly. Unauthorized software found on University assets will cause the hardware asset to be blocked from the University network until the software can be properly investigated.

A UTSI helpdesk ticket is to be created for the updating of all approved software. Software updates are to be tested on a small subset of machines before being automatically or manually applied to end user machines.

Retired or decommissioned software is to be removed from University assets as soon as end of life date is reached or license expired. An update to the centralized inventory will be made noting that the software has been removed from use.

Exceptions

Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

Related Policies

- [IT0001 – General Statement on Information Technology Policy](#)
- [IT0003 – Information Technology Security Program Strategy](#)
- [IT0004 – Information Technology Risk Management](#)
- [IT0005 – Data Categorization](#)
- [IT0017 – Information Technology Incident Response Management](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)



SPACE INSTITUTE

UT Space Institute IT Procedure: Asset Management	
Version: 1	Effective Date: 10/01/2025

- [IT0014 – Information Technology Security Awareness Training Management](#)
- [IT0311 – Information Technology Data Access, Management, and Recovery](#)
- [IT0506 – Information Technology Account and Credential Management](#)
- [IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing](#)
- [IT1516 – Information Technology Service Provider Management and Application Software Security Management](#)
- [IT4912 – Information Technology Secure Configuration Management](#)
- [IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy](#)