THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0102 - Information Technology Asset Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to create and maintain sound processes for procuring, identifying, tracking, maintaining, and disposing of all University Information Technology Assets.

II. University Hardware Asset Management Process Policy

Asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an Information Technology Asset (Asset) owned by the University. This policy does not conflict with or supersede University policies FI0600 or FI0650.

This policy provides the processes and procedures governing the University Asset lifecycle. An inventory must be created, maintained, be current, and reflect the Assets owned, operated, and managed by the University.

The Central IT Department must communicate the requirements and processes for hardware Asset management to the campus community annually to engage campus communities and individuals in the shared responsibility of Asset management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. The Central IT Department must develop a process to centrally manage all University owned Assets. The process will include at a minimum:

a. Documentation of any Asset that cannot be centrally managed and the compensating controls.

b. Utilization of the University-approved endpoint management solution (currently Intune).

c. Utilization of the current University-approved endpoint detection and response (EDR) solution. Contact the Central IT Department for guidance on the approved EDR solution and its requirements.

2. The Asset management process must include, at a minimum, the following:

a. A methodology to track the departmental and individual ownership of Assets and assign each a unique identifier.

b. A methodology to record the following information for each Asset and be prepared to provide the information promptly upon request:

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

c. The Central IT Department will create a process for University Assets not included within the inventory to be investigated, as these Assets may be unauthorized.

i. Assets owned by the University but not currently documented within the University Asset inventory must be added to the inventory.

ii. The Central IT Department must create a process for to address unauthorized Assets.

iii. The Central IT Department must create a process remove the unauthorized Asset from the IT Network, deny the Asset from connecting remotely to the IT Network, or quarantine the Asset.

d. The Central IT Department will create a process for verification, at least annually, of each Asset that is completed in-person or remotely unless an exemption is authorized by the dean or department head.

3. Information Technology Asset Custodians are required:

a. To connect the University's Assets to the University IT Network on a weekly basis, where practical. Permanently air-gapped (Systems that do not connect to the University's Resources) Assets must be approved by the Central IT Department.

a. To maintain control over the University Assets.

b. To use the process defined by the Central IT Department to gain assistance with any problems such as malfunctions, needed repairs, and underutilized equipment or in the event of the loss of an Asset.

4. Controlled Disposal

a. Assets to be decommissioned or retired must be returned using the process defined by the Central IT Department.

b. The Central IT Department will create a process for:

i. The secure erasure of the primary memory storage device within the University Asset, where applicable.

ii. The campus community to update the status of the University Assets within all University management Systems.

iii. Ensuring that records are retained in compliance with the Record Retention Policy.

iv. Documenting the removal of the University Asset from the University within the Asset inventory.

5. Uncontrolled Disposal

a. All lost or stolen University Assets must be immediately reported to the appropriate business units, including the Central IT Department, and the campus or institute CISO/DISL. Reference University Policy: FI0131 – Cash Shortages and Property Losses for more information.

b. A report must be filed with law enforcement for all University IT Assets assumed stolen.

c. Lost or stolen University Assets must have their access to University Data revoked as soon as possible. The Data Owner must also be notified if University Data is present on the Asset.

d. The Central IT Department will create a process for:

i. Updating the status of the University Assets within all University management Systems.

ii. Initiating remote secure erasure for devices that are determined to be lost or stolen and contain Protected University Data. The Data Owner must be notified if Protected University Data is present on the Asset.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

6. The Central IT Department will utilize an active discovery tool to identify Assets connected to the University's IT Network (IG2). This includes configuring an active discovery tool to execute daily.
7. The Central IT Department will use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the University's IT Asset inventory (IG2). This includes reviewing use logs to update the University's Asset inventory weekly.
8. The Central IT Department will use a passive discovery tool to identify IT Assets connected to the University's IT Network. Review and use scans to update the University's Asset inventory at least weekly (IG3).

III. University Software Asset Management Process Policy

Software IT Asset management is the process of procuring, identifying, tracking, maintaining, and removing University procured software on University IT hardware Assets. This policy provides guidance for governing the software Asset lifecycle while the University is using a software Asset. A software inventory must be created and maintained to support the University's mission and to help ensure only authorized software is installed and used. This software inventory must be up-to-date and reflect the current state of software across the University.

For software developed by University personnel for University use, reference System-wide Policy IT1516 - Information Technology Service Provider Management and Application Software Security Management.

The Central IT Department must communicate the requirements and processes for software Asset management to the campus community annually to engage campus communities and individuals in the shared responsibility of Asset management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

All Users should contact the Central IT Department if they have special software needs that do not follow the established guidelines of this policy to determine if any software Assets need to be added to the official software Asset list.

1. Software Asset management begins with clearly defining the procurement process to ensure all software is reviewed for appropriate security controls. This includes the requirements that:

a. The Central IT Department will create a process, in conjunction with the Procurement Office, for procurement of software that includes a defined approval process.

b. The Central IT Department must maintain a list of approved software vendors. A User or Unit should, prior to procurement, contact the Central IT Department for approval of the vendor. Software must only be purchased from vendors on the University's approved vendor list.

2. Any software installed on University hardware Assets, alongside other relevant information within the software Asset, must be recorded within the software inventory. This must include:

a. Title of software

b. Developer or publisher of software

c. Version

d. Date of acquisition

e. Business purpose

f. Uniform Resource Locator (URL)

g. End-of-support (EoS) date, if known

h. End-of-life (EoL) date, if known

i. Any relevant licensing information

j. Decommission date

k. Software Asset Custodian

3. The Central IT Department will create a process to verify the software IT Asset inventory at least annually, or more frequently as needed.

a. Only software that has been approved by The Central IT Department may be installed on University hardware Assets.

b. Only cloud services that have been approved by The Central IT Department may be used for University business.

i. University-owned mobile devices may only obtain software from The Central IT Department approved sources.

4. The Central IT Department will create a process to review all software installed on University hardware Assets at least bi-annually.

a. All installed software on University hardware Assets must be reported to the Central IT Department on a regular basis.

b. All newly discovered software must be checked against the list of approved software in the software Asset inventory.

5. Identified software not included within this inventory must be investigated as the software may be unauthorized.

a. Hardware Assets containing unauthorized software must be removed from the IT Network unless temporary access is granted by The Central IT Department.

b. The presence of unauthorized software must be properly investigated.

c. All newly discovered (authorized) software must be added to the software inventory.

d. Unauthorized software must be removed from use on University hardware IT Assets or receive a documented exception.

6. A process to approve all updates and upgrades must be created by The Central IT Department prior to installation. The Central IT Department will ensure, in partnership with unit staff where present, that managed devices are configured to receive automatic updates, or that users have the necessary instructions to do so, which constitutes tacit approval.

7. The Central IT Department will create a process for the removal of software Assets that adheres to the following:

a. Provides guidance for the campus community for software Assets to be decommissioned, for example licensing, to be removed from all University hardware IT Assets.

b. Ensures hardware Assets containing retired software are protected with additional defensive mitigations, such as removal from the IT Network or isolation.

c. Ensures that University Data is copied to a secure Data repository prior to the removal of the software. Contact the Data Owner or Data Custodian for more information on the protections required for the copied Data.

d. Ensures that retired software does not store Data in other servers or cloud infrastructure not owned by the University.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

8. The Central IT Department will create a process or processes to:

a. Utilize software inventory tools, when possible, throughout the University to automate the discovery and documentation of installed software (IG2).

b. Use technical controls, such as application allow listing, to ensure that only authorized software can execute or be accessed (IG2) and reassess the use bi-annually at a minimum.

c. Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a System process (IG2) including blocking unauthorized libraries from loading into a System process and reassessing bi-annually at a minimum.

d. Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute (IG3) including blocking unauthorized scripts from execution and reassessing bi-annually at a minimum.

IV. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for Information Technology Asset management as described in CIS Control 1 (Inventory and Control of University Assets) and CIS Control 2 (Inventory and Control of Software Assets) for the University of Tennessee in support of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy 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 policy 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.

SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

---

SECTION 8. Policy History

Revision 1:

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0005 – Data Categorization

f. IT0014 – Security Awareness Training Management

g. IT0017 – Information Technology Incident Response Management

h. IT0311 – Information Technology Data Access, Management, and Recovery

i. IT0506 – Information Technology Account and Credential Management

j. IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing

k. IT1516 – Information Technology Service Provider Management Application Software Security Management

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/
