THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0102-HSC-A Asset Management	
Version 6	**Effective Date: 09/30/2017**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

For the University of Tennessee Health Science Center (UTHSC) leadership to make informed, business-driven decisions regarding computing assets, they must first know what assets exist, and the status of those assets. This information provides UTHSC visibility into license utilization, software support costs, unauthorized devices, vulnerabilities, threats, and compliance posture. This Standard establishes requirements for the management of UTHSC IT Resources.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This Standard applies to all UTHSC IT Resources, regardless of physical location.

Definitions

Center for Internet Security (CIS) Critical Control #1 - Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Center for Internet Security (CIS) Critical Control #2 - Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Enterprise assets – assets with the potential to store or process data. Enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.
UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.
Software assets – programs and other operating information used within an enterprise. Software assets include operating systems and applications.

Responsibilities

Executive Leadership of ITS or designee is responsible for the development of an asset management program that incorporates the fundamentals of the Center for Internet Security (CIS) Critical Controls 1 and 2.
Chief Information Security Officer (CISO) or designee is responsible for consulting with the CIO on security controls required as part of the asset management program.
UTHSC End User (Asset Custodian) is responsible for maintaining the IT Resources assigned to them. This includes using TechConnect to gain assistance with any problems, such as malfunctions, needed repairs, or security-related incidents. This also includes keeping devices powered on and available to receive updates in a timely manner and following the University of Tennessee's Acceptable Use Policy (IT0002) and UTHSC's IT0002-HSC-A-Acceptable Use of IT Resources.

Standard

UTHSC Inventory and Controls of Enterprise Assets (CIS 1)

- Information Technology Services (ITS) will establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets.
- At a minimum, the inventory should record:
  - University Asset Identifier
  - Network address (if static)
  - Hardware address
  - Name of the asset custodian and role (administrator, user)
  - Department for each asset
  - Physical location where applicable
  - Serial number if applicable

  - Item description
  - Approval to connect to the network (Y/N)
- This inventory includes assets connected to the infrastructure physically, virtually, remotely, and within cloud environments.
- It also includes assets that are regularly connected to UTHSC's network infrastructure, even if they are vendor or 3rd party managed.
- This inventory is updated whenever an asset is installed, removed or the system is updated.
- Unauthorized assets must be detected and evaluated. Network access is disabled for these devices.
- Verification of these assets must be completed at least annually.
- Refer to IT0102-HSC-B-Device Life Cycle Security for the security maintenance of IT Resources throughout the life of the asset.

UTHSC Inventory and Controls of Software Assets (CIS 2)

- ITS will establish and maintain a detailed inventory of all licensed software installed on enterprise assets.
- At a minimum, the inventory must include:
  - Title of software
  - Developer or publisher of software
  - Version
  - Date of acquisition
  - Business purpose
  - Uniform Resource Locator (URL)
  - End-of-support (EoS) date, if known
  - End-of-life (EoL) date, if known
  - Any relevant licensing information
  - Decommission date
  - Software Asset Custodian
- This inventory is updated whenever an asset is installed, removed or the system is updated. It should be verified at least annually.
- All software installed on IT Resources should be reviewed at least biannually.
- Unauthorized software and firmware must be detected and evaluated.

    - Hardware assets containing unauthorized software must be removed from the UTHSC network until evaluation.
- Refer to IT0102-HSC-B-Device Life Cycle Security for the security maintenance of software on IT Resources throughout their life cycle.

As UTHSC IT Resources inclusive of data and information are the property of the University of Tennessee and their use is intended for authorized use for the University of Tennessee only, the UTHSC possesses the exclusive right to manage and direct actions regarding those UTHSC IT Resources in accordance with UTHSC and University of Tennessee policies and procedures so long as asserting and exercising this right does not conflict with federal or state law or regulations.

UTHSC IT Resources are classified in terms of their value, legal requirements, sensitivity, and criticality to the UTHSC. Data and systems are classified in accordance with IT0005-HSC-A-Data & System Categorization.

References

1. IT0002-Acceptable Use of Information Technology Resources
2. IT0102-Information Technology Asset Management
3. IT0002-HSC-A-Acceptable Use of IT Resources
4. IT0005-HSC-A-Data & System Categorization
5. IT0102-HSC-B-Device Life Cycle Security