THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: GP-007-Asset Management	
Version 5	**Effective Date: 09/30/2017**

Responsible Office: Office of Cybersecurity	Last Review: 07/10/2023 Next Review: 07/10/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

For 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.

Information Technology (IT) Resources – The collection of data and technology that support the achievement of organizational goals. IT Resources include hardware, software, vendors, users, facilities, data systems, and data.
Software assets – programs and other operating information used within an enterprise asset. Software assets include operating systems and applications.

Responsibilities

Chief Information Officer (CIO) 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 Office (CISO) or designee is responsible for consulting with the CIO on security controls required as part of the asset management program.
UTHSC End User is responsible for maintaining the IT Resources assigned to them. This includes keeping devices powered on and available to receive updates in a timely manner and following the University of Tennessee's Acceptable Use Policy (IT0110) and UTHSC's GP-004-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:
  - network address (if static)
  - hardware address
  - machine name
  - asset owner
  - department for each asset
  - serial number if applicable
  - 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.

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 will document each entry's title, publisher, initial install/use date, and business purpose.
    - Where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.
- This inventory is updated whenever an asset is installed, removed or the system is updated.
- Unauthorized software and firmware must be detected and evaluated.

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 GP-002 Data & System Classification.

References

1. UTSA IT0110-Acceptable Use of Information Technology Resources
2. CS-001 Device Life Cycle Security
3. GP-002 Data & System Classification
4. GP-004-Acceptable Use of IT Resources

UT Health Science Center: GP-007-Asset Management	
Version 5	**Effective Date: 09/30/2017**