THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0002-HSC-A Acceptable Use of IT Resources	
Version 4	**Effective Date: 04/29/2020**

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

The University of Tennessee Health Science Center (UTHSC or University) Acceptable Use Policy (AUP) regulates UTHSC computing resources usage.

Scope

All UTHSC persons who access the UTHSC network or computers and technology.

Definitions

Antivirus/Antimalware - A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.

Encryption - a method by which information is converted into cipher code that hides the information's true meaning

Restricted Data: The effect on confidentiality and integrity of the Data is significant and includes compliance requirements. This Data is governed by federal, or state compliance requirements and unwarranted exposure can lead to compliance issues and/or fines. This includes all Data that contains personally identifiable information (PII), protected health information, student education records, and cardholder Data. This categorization level also includes lower-risk items that, when combined, represent increased risk. per IT0005-HSC-A-Data & System Classification. Minimum security requirements are explained on the webpage https://uthsc.edu/its/cybersecurity/requirements.php.

Standard

UTSA IT Policy IT002-Acceptable Use of Information Technology Resources **is the superseding document to this Standard. The following are additions or clarifications to specific sections of that policy.**

IV.2 Users Will

- Ensure their devices on the UTHSC network have antivirus/antimalware protection.

- By logging into UTHSC computers acknowledge they understand and agree to the acceptable use standards of UTHSC, the acceptable use policy of the University of Tennessee which is further communicated by the banner notice when logging into UTHSC systems.
- Must gain owner's permission to access (e.g., read, write, modify, delete, copy, move) the owner's files or electronic mail, regardless of whether the operating system allows this access to occur.
- To protect and secure data that needs Level 2 security, the user must adhere to the UTHSC Encryption standard, IT0311-HSC-E-Encryption.
- If at any time a user receives an email or instant message that places the user and/or the user's information at risk or leads the user to believe that a criminal act may be pending, the user should immediately report the matter to campus police or local authorities at (901) 448-4444 or campuspolice@uthsc.edu
- Encrypt protected data or data that needs level 2 security when sending such data, such as SSN or credit card information, either by using encrypted email or the UT Vault.

IV.3 Users Will Not

- Respond to electronic requests (email, instant message, text message, etc.) that ask for generally protected information, such as passwords, social security numbers, or credit card numbers.

VI. Personal Use

- All personally owned devices used to store, process, or transmit university information or those otherwise connected to University resources are subject to the regulations of acceptable use.

VII. Misuse of IT Resources

- Appropriate authorities (e.g., appropriate office for student conduct matters, UT Human Resources, UT General Counsel, the police department with campus jurisdiction) or local and federal law enforcement agencies will be notified of any misuse.

UT Health Science Center: IT0002-HSC-A Acceptable Use of IT Resources	
Version 4	**Effective Date: 04/29/2020**

Policy History

Version #	Effective Date
1	04/29/2020
2	05/13/2022
3	01/11/2023
4	03/01/2025 – new naming convention

References

1. IT0002-Acceptable Use of Information Technology Resources
2. IT0005–Data Classification
3. IT0005-HSC-A-Data & System Classification
4. IT0311-HSC-A.06-Third-Party Access to Accounts and Data
5. IT0311-HSC-E-Encryption
6. https://uthsc.edu/its/cybersecurity/requirements.php
7. NIST: Glossary of Key Information Security Terms