THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: GP-004-Acceptable Use of IT Resources	
Version 3	**Effective Date: 04/29/2020**

Responsible Office: Office of Cybersecurity	Last Review: 01/11/2023 Next Review: 01/11/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

University of Tennessee Health Science Center (UTHSC or University) Acceptable Use Policy (AUP) regulates the use of UTHSC computing resource. 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

All UTHSC persons who access 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.

Level 3 Data: The security level needed for data defined by UTHSC Standards whose unauthorized disclosure could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UTHSC students, patients, research subjects, employees, guests/program participants, UTHSC reputation, or the overall operation of the Location or essential services. This classification level also includes lower risk items that, when combined, represent increased risk. per GP-002-Data & System Classification. Minimum security requirements are explained on the webpage https://uthsc.edu/its/cybersecurity/requirements.php.

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

UT Health Science Center: GP-004-Acceptable Use of IT Resources	
Version 3	**Effective Date: 04/29/2020**

Standard

UTSA IT Policy IT0110 - Acceptable Use of Information Technology Resources is the superseding document to standard. The following are additions or clarifications to specific sections of that policy.

1. Privacy
   - The University cannot guarantee the privacy of files, electronic mail, or other information stored or transmitted on University resources.
   - The University cannot promise privacy of information stored on or sent through University-owned information systems and communications infrastructure except for certain records relating to students; research; proprietary, trade secret or patentable materials; or certain medical records.

2. Users Will
   - Ensure their devices on the UTHSC network have antivirus/antimalware protection. UTHSC owned devices are installed with CarbonBlack. MalwareBytes is available for download personal devices for students.
   - 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 3 security, the user must adhere to the UTHSC Encryption standard.
   - 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 3 security when sending such data, such as SSN or credit card information, either by using encrypted email or the UT Vault.

3. Users Will Not
   - Use resources for illegal or obscene activity
   - Although not an inclusive list, examples of illegal or obscene use include theft, fraud, gambling, copyright infringement, sound, or video recording piracy, and either viewing or distributing child pornography.
   - 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.

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

7. Misuse of IT Resources
   - Notification will be made to the 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.

References

1. UTSA IT Policy IT0110 - Acceptable Use of Information Technology Resources
2. UTSA IT Policy IT0115 – Information and Computer System Classification
3. GP-002-Data & System ClassificationAC-001.06-Third-Party Access to Account and DataSC-005-Encryptionhttps://uthsc.edu/its/cybersecurity/requirements.php
4. NIST: Glossary of Key Information Security Terms