TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 56.01, **Acceptable Use of Information Technology Resources**

PURPOSE: The purpose of this Operating Policy (OP) is to define the acceptable use of all Texas Tech Health Sciences Center (TTUHSC) computers, information and information systems. This policy outlines general compliance instructions and communicates acceptable and non-acceptable activities for which institutional information and information systems can be utilized.

REVIEW: This OP will be reviewed annually in July by the Vice President of Information Technology and Chief Information Officer (CIO), the Assistant Vice President of Information Security and Information Security Officer (ISO), and the Assistant Vice President of Technology Services.

TABLE OF CONTENTS

POLICY

1. Information and Information Systems Acceptable Use Responsibility

TTUHSC's information and information systems are owned by the State of Texas and administered by the IT (Information Technology) Division. TTUHSC will provide access to appropriate resources to all members of the TTUHSC community. Employee, student, and third-party users are responsible for managing their use of information and information systems and are also held accountable for their actions relating to IT security. By logging into TTUHSC systems, users acknowledge and agree to comply with all applicable TTUHSC IT policies.

a. Approved Access

Some TTUHSC positions and related activities require access to resources critical to computer security and privacy. TTUHSC may require these users to participate in special training or complete required forms.

b. Authorized Access and Security Programs Authority

Users may use only the information and information systems to which they have been given authorized access. Users must not attempt to access any data or programs their supervisor has not given authorization or explicit consent to access.

2. Acceptable Use of AI

The use of AI with TTUHSC information and information systems is covered in HSC OP 52.21 Acceptable Use of Artificial Intelligence (AI) Tools

3. System Usage

a. Reasonable Personal Use of Computer and Communications Systems

TTUHSC information and information systems are provided for the express purpose of conducting the business of TTUHSC. However, as a convenience to the TTUHSC user community, incidental use of information and information systems is permitted. All personal use must be consistent with all TTUHSC policies.

b. Prohibited Use of Computer and Communications Systems

Users may not access websites or use applications that appear on the State of Texas Prohibited Technologies list as outlined in HSC OP 56.06 Prohibited Technologies. Additional sites may be blocked from access depending on potential risk to TTUHSC systems. In addition, prohibitions on use are defined as follows.

(1) Incidental personal use must not result in direct or indirect costs to any TTUHSC institution.

(2) Incidental personal use must not interfere with the normal performance of an employee's job duties.

(3) No files or documents may be sent or received that may cause legal action against any institution in the Texas Tech University (TTU) System.

(4) Incidental use of information and information systems is restricted to approved users and does not extend to family members or acquaintances.

(5) Users are prohibited from using the TTUHSC systems or networks for personal or commercial gain. This includes:

i. Selling access to your user ID or to TTUHSC systems or networks.

ii. Performing work for profit with TTUHSC resources in a manner not authorized by TTUHSC.

iii. Marketing and advertising not authorized by the TTUHSC Communication and Marketing Director.

iv. Storing personal email messages, voice messages, files, and documents (beyond a minimal amount) within any institutional information and information system.

(6) TTUHSC systems are not to be used for circulating messages in violation of TTUHSC OP's or System Regulations. See TTUHSC OP 51.02 Non-Discrimination and Anti-Harassment Policy and Complaint Procedure and Texas Tech System Regulation 10.01, which includes two distinct policies and procedures based on applicable federal and state law: 10.01 A Title IX Sexual Misconduct and 10.01 B Non-Title IX Sexual Misconduct. In addition, TTUHSC systems must not be used for partisan political purposes (e.g., using email to circulate advertising for political candidates or lobbying for public officials).

NOTE: All messages, files and documents-including personal messages, files and documents-located on institutional information systems are owned by the institution, may be subject to open records requests, and may be accessed in accordance with this policy.

c. Unreasonable Interference

Users must not unreasonably interfere with the fair use of information and information systems. This includes, but is not limited to:

(1) Playing games.

(2) Listening to, viewing, or streaming audio/video.

a. To ensure business critical processes are not affected by resource demands, users must not subscribe to or continuously display streaming media services except for occasional, short term or educational usage.

b. Unauthorized persistent streaming usage will result in termination of access.

(3) Intentionally misconfiguring or tampering with videoconferencing equipment.

(4) Interfering with the scheduled use of a distance learning classroom by failing to promptly vacate the room at the end of a session.

(5) Intentionally running a program that attempts to violate the operational integrity of the TTUHSC network.

d. Use at Your Own Risk

Users access the internet through TTUHSC facilities at their own risk. TTUHSC is not responsible for material viewed, downloaded, or received by users through the internet as websites or email systems have the potential to deliver offensive content.

e. Activity Monitoring, User Privacy, and Investigations

Users must be aware that while using TTUHSC systems, their internet activity is monitored and recorded. This information may include, but is not limited to:

(1) Websites visited.

(2) Files downloaded.

(3) Time spent on the internet.

(4) Users of state property have no expectation of privacy for information created on or contained therein. TTUHSC is required to disclose the contents of electronic files when required for legal inquiries, audits, or legitimate federal, state, local, or institutional purposes.

NOTE: All messages, files, and documents (including those of a personal nature) located on institutional information and information systems are owned by the institution, may be subject to open records requests, and may be accessed in accordance with this policy.

(5) All authorized users shall cooperate with official state and federal law enforcement authorities in aiding the investigation and prosecution of any suspected infraction of security and privacy statutes or policies involving either TTUHSC personnel or TTUHSC computing facilities.

f. Unattended Active Sessions

Users must not leave their personal computer, workstation, or terminal unattended without logging out or utilizing a password-protected screen saver. If sensitive information resides on a computer, the screen must immediately be locked, or the machine turned off, whenever a user leaves the location where the computer is in use.

g. Session Timeout

Sessions left inactive for 15 minutes will cause the screen to automatically lock, obscuring the contents of any open windows or files.

4. User IDs and Passwords

Passwords are considered confidential information and must not be shared with anyone including IT personnel or administrative assistants.

a. Personal User ID Responsibility

Users are responsible for all activity performed with their personal user IDs. Users must not permit anyone to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.

b. Access Code Sharing

TTUHSC accounts, user IDs, passwords, voice mailbox personal identification numbers, and any other identifiers/access codes must not be used by anyone other than the person to whom they were originally issued.

c. Sharing Passwords

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. IT staff will never ask users to share or reveal their passwords.

d. Suspected Password Disclosure

If a user suspects their eRaider account has been compromised, or, their password is disclosed to an unauthorized third party, they must immediately change their password and then contact the IT Solution Center (ITSC) for assistance to mitigate any impact that may occur.

e. Password Security

(1) Strong Passwords

Users must choose passwords that are difficult to guess. Criteria and guidelines for creating a strong password can be found in the TTUHSC IT Password Standard.

(2) Entering Passwords Safely

Users must never type their passwords at a keyboard or a telephone keypad if they are aware of someone watching their actions which may expose the information and lead to unauthorized access.

(3) Password Proximity to Access Devices

Users must never write down or otherwise record a readable password and store it near the device on which it is used.

5. Essential and Least Privilege

TTUHSC configures information systems to provide only essential capabilities. To ensure only essential capabilities are provided, the principle of least privilege is applied for access to applications and systems.

Users with essential or elevated privileges have a greater responsibility to the Institution to ensure the

secure operation of any TTUHSC system. As a result, users with essential or elevated privileges are held to a higher standard for disciplinary action.

6. Electronic Communication

All use of TTUHSC electronic communication should follow the relevant policies and procedures for usage as represented by HSC OP 56.04 Data Security and Privacy and TTUHSC IT Policy 56.22 Email,

a. Identity Misrepresentation

Users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any TTUHSC electronic communications.

b. Handling Attachments

All email attachment files from third parties are automatically scanned with a TTUHSC-authorized virus detection system.

c. No Guarantee of Message Privacy

TTUHSC cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users must be careful about the topics covered in TTUHSC electronic communications and should use discretion when transmitting messages.

d. Outbound Email Footer

Users should include, in outbound emails, a footer that refers to the possibility that the message may contain confidential information and that it is for the use of the named recipients only.

e. Responding to Messages

If users receive messages in violation of this policy, the must immediately forward them to the Information Technology Solution Center (ITSC).

f. Messages in Violation of Other University Policies

TTUHSC's policies, including but not limited to policies addressing harassment apply to the use of information and information systems. Please refer to TTUHSC OP 51.02 Non-Discrimination and Anti-Harassment Policy and Complaint Procedure and Texas Tech System Regulation 10.01, which includes two distinct policies and procedures based on applicable federal and state law: 10.01 A Title IX Sexual Misconduct and 10.01 B Non-Title IX Sexual Misconduct.

7. Internet and Web Usage

a. Posting Sensitive Information

Users must not post unencrypted TTUHSC material on any publicly accessible computer unless the posting of these materials has been approved by the Office of Communications and Marketing.

b. Disclosing Internal Information

Users must follow TTUHSC OP 67.03 Use of Social Media when posting to any website, including blogs, newsgroups, chat groups, or social networking sites. Such information includes business prospects, unpublished research data, and internal information systems problems.

c. Compliance with Applicable Laws and University Policies

TTUHSC is not responsible for content that users may encounter while using the internet. Users are responsible for ensuring that their use of the internet and access to the web is consistent with applicable laws and university policies.

d. Blocking Sites and Content Types

The ability to connect with a specific website does not in itself imply that users of TTUHSC systems are permitted to visit that site. TTUHSC may, at its discretion, restrict or block the downloading of certain file types and access to malicious sites that are likely to cause network service degradation (e.g., graphics, video, and music files).

8. Data Storage

a. Establishing Third-Party Networks

Users must not establish any third-party information storage network that will handle TTUHSC information (e.g., electronic bulletin boards, blogs, cloud storage) without the approval of the IT Division.

9. Internal Systems

a. Eradicating Computer Viruses

Any user who suspects their machine has been infected by a virus or malicious software must immediately contact the ITSC. Attempts must not be made to eradicate the virus without assistance from the IT Division.

b. Trusted Software Scanning

Users must not use any externally-provided software from a person or organization other than a TTUHSC-known and trusted supplier, unless the software has been scanned for malicious code and approved by the IT Division.

c. Material That Violates Law or University Policy

Users must comply with federal and state laws and university policies. Please refer to

TTUHSC OP 51.02 Non-Discrimination and Anti-Harassment Policy and Complaint Procedure and Texas Tech System Regulation 10.01, which includes two distinct policies and procedures based on applicable federal and state law: 10.01 A Title IX Sexual Misconduct and 10.01 B Non-Title IX Sexual Misconduct.

(1) Using sexually explicit material to intimidate, persecute, or harass is illegal and is sexual harassment. For detailed guidelines on sexual harassment, refer to TTUHSC OP 51.02 Non-Discrimination and Anti-Harassment Policy and Complaint Procedure

(2) Do not open any emails you believe to contain obscene content or pornography. If obscene content or pornography is received through email, there will be no disciplinary proceedings if the mail is deleted immediately. If the offending email originates from a TTU or TTUHSC email address, report it to the TTUHSC Title IX Coordinator immediately by phone at (806) 743-9861, or, by email at TitleIXCoordinator@ttuhsc.edu.

d. Copyrighted and Authorized Software

(1) Use only legal versions of copyrighted software and materials (including music, movies, and other media) in compliance with vendor license requirements.

(2) Users shall not install any software provided by TTUHSC to non-TUHSC owned devices without prior authorization from the IT Division. Software is licensed to your assigned work device(s) only. Installation without proper authorization constitutes theft.

(3) Users must not make unauthorized copies of copyrighted software.

(4) Users must not use any type of unauthorized software listed in the Authorized and Unauthorized Hardware/Software Standard without the explicit approval of the CIO or the CIO's designee.

e. Computer Viruses

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any TTUHSC computer or network.

f. External Storage

All removeable storage media that users connect to TTUHSC machines must be encrypted as described in the Data Storage Standard..

10. Personal Equipment

Use of personal phones, laptops, desktops, and tablets are not allowed for the creation and storage of TTUHSC information. Only email may be accessed from personal machines.

a. User Installation of Software

Users must not install software owned by TTUHSC on their personal devices without receiving advance authorization to do so from the IT Division.

b. Unattended Active Sessions

If a personal computer system which is connected by Remote Desktop or VPN to a TTUHSC system, users must not leave that personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

11. Unauthorized Use

For a detailed discussion of unauthorized and prohibited hardware and software, please see the Authorized/Unauthorized Hardware-Software Standard.

a. Non-authorized VPN

Non-authorized or privacy VPNs are not allowed to access TTUHSC systems. Only TTUHSC-requested and approved VPN may be used to remotely access TTUHSC networks.

b. Peer-to-Peer Programs

(1) Use of all peer-to-peer (P2P) programs (e.g., BitTorrent) on TTUHSC computers or the TTUHSC network for the purpose of downloading or uploading illegal copies of copyrighted media is strictly prohibited.

(2) Any computers using P2P applications on the TTUHSC network are subject to removal from the network until the application is removed or disabled.

c. Authorized Access and Security Programs Authority

A user must not download, install, or run programs or utilities that reveal or exploit weaknesses in the security of a system unless the individual user has explicit written consent from the institution's ISO. Such programs include, but are not limited to:

(1) Password cracking programs

(2) Packet sniffers

(3) Port scanners

(4) Any operating systems designed for discovering and exploiting vulnerabilities, (e.g., Kali Linux)

(5) Any unapproved programs on TTUHSC information systems.

d. Circumventing or Subverting TTUHSC Systems

Users must not attempt to circumvent or subvert the system or the network, destroy the integrity of computer-based information, or access-controlled information on the TTUHSC network.

e. Bring-Your-Own-Device (BYOD)/Guest Wireless Network

Non-TTUHSC-owned computers connecting to the HSC-Air network will automatically be redirected to the BYOD/guest wireless network. Those networks cannot be used to complete TTUHSC business-related activities. TTUHSC-owned devices are not permitted on the BYOD/Guest network and may be disconnected without notice by the ISO.

12. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. TTUHSC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

a. Disciplinary Repercussions

Misuse of TTUHSC Information or Information Systems is a violation of the policies contained herein and can result in disciplinary action in accordance with, but not limited to, TTUS Regulation 10.07 Employee Conduct, Coaching, Corrective Action, and Termination and HSC OP 77.05 Suspension and Retention, as well as the Student Handbook.

13. Related Statutes, Policies, and Requirements

Digital Millennium Copyright Act
Digital Millennium Copyright Act of 1998

Health Insurance Portability and Accountability Act
HIPAA, Title 45, Subtitle A, Subchapter C, Part 164

Payment Card Industry (PCI) Data Security Standard (DSS)
PCI-DSS: 12.2 Acceptable Usage

Texas Administrative Code
TAC 477, Subchapter C, 70-76

Texas Public Information Act
Texas Public Information Act

TXCC Security Control Standards Catalog
Texas Cyber Command Security Control Standards Catalog

TTUHSC IT Areas of Responsibility
Information and Information System Roles and Responsibilities

Document Details

Approval and Ownership

Approved By	Vince Fell
Title	Vice President for Information Technology and Chief Information Officer
Approval Date	9/6/2017
Owner(s)	IT Executive Management Team

Revision History

Version	Description	Date Reviewed	Date Submitted for Publishing	Reviewer(s)
1.0	Initial version	N/A	2/27/2015	N/A
2.0	Annual review	N/A	2/3/2016	N/A
3.0	Annual review	8/15/2017 8/30/2017	9/15/2017	HIPAA Privacy and Security Committee IT Executive Management Team
4.0	Annual review	12/03/2018	1/09/2019	Vice President for Information Technology and Chief Information Officer
5.0	Annual review	7/29/2019	7/31/2019	Vice President for Information Technology and Chief Information Officer and the IT Director of Policy and Planning
6.0	Annual review	8/14/2020	8/28/2020	Vice President for Information Technology and Chief Information Officer and the IT Director of Policy and Planning
7.0	Annual review	7/22/2022	8/01/2022	Vice President for Information Technology and Chief Information Officer and Information Security Officer
8.0	Annual review	5/25/2023		Vice President for Information Technology and Chief Information Officer and Information Security Officer
9.0	Annual review	07/07/2025		Vice President for Information Technology and Chief Information Officer and Information Security Officer