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 and Information Resource (IR) assets. This policy outlines general compliance instructions and communicates acceptable and non-acceptable activities for which institutional IR can be utilized.

REVIEW: This OP will be reviewed annually in July by the TTUHSC Chief Information Officer (CIO).

TABLE OF CONTENTS:

1. Information Resources Acceptable Use Responsibility 3
a. Approved Access 3
b. Authorized Access and Security Programs Authority 3
2. System Usage 3
a. Reasonable Personal Use of Computer and Communications Systems 3
b. Prohibited Use of Computer and Communications Systems 3
c. Unreasonable Interference 4
d. Use at Your Own Risk 4
e. Activity Monitoring, User Privacy, and Investigations 4
f. Unattended Active Sessions 4
g. Session Timeout 5
3. User IDs and Passwords 5
a. Personal User ID Responsibility 5
b. Access Code Sharing 5
c. Sharing Passwords 5
d. Strong Passwords 5
e. Typing Passwords When Others are Watching 5
f. Password Proximity to Access Devices 5
4. Electronic Communication 6
a. Identity Misrepresentation 6
b. Handling Attachments 6
c. No Guarantee of Message Privacy 6
d. Outbound Email Footer 6
e. Responding to Offensive Messages 6
f. Harassing or Offensive Materials 6
5. Internet and Web Usage 7
a. Posting Sensitive Information 7
b. Disclosing Internal Information 7

c. Offensive Websites 7
d. Blocking Sites and Content Types 7
6. Data Storage 7
a. Establishing Third-Party Networks 7
7. Internal Systems 7
a. Eradicating Computer Viruses 7
b. Trusted Software Scanning 7
c. Sexually Explicit Material 8
d. Copyrighted and Authorized Software 8
e. Computer Viruses 8
f. External Storage Checking 8
8. Personal Equipment 9
a. User Installation of Software 9
b. Unattended Active Sessions 9
9. Unauthorized Use 9
a. Peer-to-Peer Programs 9
b. Authorized Access and Security Programs Authority 9
c. Circumventing or Subverting TTUHSC Systems 9
d. Guest Wireless Network 9
10. Violations 10
a. Disciplinary Repercussions 10
Related Statutes, Policies, and Requirements 11
Document Details 12

POLICY:

1. Information Resources Acceptable Use Responsibility

TTUHSC's IR 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 IR and are also held accountable for their actions relating to IT security.

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 IR 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. System Usage

a. Reasonable Personal Use of Computer and Communications Systems

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

b. Prohibited Use of Computer and Communications Systems

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 or embarrassment to any institution in the Texas Tech University (TTU) System.

4) Users of state-owned IR shall have no expectation of privacy except as otherwise provided by applicable privacy laws.

5) Incidental use of IR is restricted to approved users and does not extend to family members or acquaintances.

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

a) Selling access to your user ID or to TTUHSC systems or networks.
b) Performing work for profit with TTUHSC resources in a manner not authorized by TTUHSC.
c) Marketing and advertising not authorized by the TTUHSC Communication and Marketing Director.
d) Storage of personal email messages, voice messages, files, and documents within any institutional IR must be nominal.
e) All messages, files and documents—including personal messages, files and documents—located on institutional IR 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 IR. This includes, but is not limited to:

1) Playing games.

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

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.

6) TTUHSC systems are not to be used for partisan political purposes (e.g., using email to circulate advertising for political candidates or lobbying for public officials).

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. All messages, files, and documents (including those of a personal nature) located on institutional IR 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

A 15-minute timeframe has been established for users to obscure the contents of their computer screens when inactive.

3. User IDs and Passwords

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 computer accounts, user IDs, network passwords, voice mailbox personal identification numbers, credit card numbers, and other 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 reveal their passwords.

d. Strong Passwords

Users must choose passwords that are difficult to guess. For example, users must not choose a dictionary word, derivatives of user IDs, common character sequences, details of their personal history, a common name, or a word that reflects work activities. For further criteria and guidelines on creating a strong password please reference TTUHSC IT policy 56.08 "Passwords and Authentication."

e. Typing Passwords When Others are Watching

Users must never type their passwords at a keyboard or a telephone keypad if they are aware of someone watching their actions. To do so unduly exposes the information accessed, thereby leading to unauthorized access.

f. Password Proximity to Access Devices

Users must never write down or otherwise record a readable password and store it near the access device to which it pertains.

g. Suspected Password Disclosure

Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

4. Electronic Communication

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 will automatically be scanned with an authorized virus detection software package.

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. Additional information about this process can be obtained from the IT Solution Center (ITSC).

d. Outbound Email Footer

A footer prepared by the TTUHSC Office of Communications and Marketing must be automatically appended to all outbound email originating from TTUHSC email accounts, including original emails and replies to messages. This footer must make reference to the possibility that the message may contain confidential information that it is for the use of the named recipients only, that the message has been logged for archival purposes, and that the message may be reviewed by parties at TTUHSC other than those named in the message header. In addition, it must be noted that the message does not necessarily constitute an official representation of TTUHSC. Additional details related to the creation of this email footer can be found in the ITSC Solve IT knowledge base under the topic “How to: Create an email signature in Microsoft Outlook 2016.”

e. Responding to Offensive Messages

Users must not respond directly to the originator of offensive email messages, telephone calls, or other forms of communication. Instead, report these instances to the ITSC.

f. Harassing or Offensive Materials

TTUHSC’s policies, including but not limited to policies addressing harassment apply to use of IR. Please refer to TTUHSC OP 51.02 “Non-Discrimination and Anti-Harassment Policy and Complaint Procedure for Violations of Employment and Other Laws” and TTUHSC OP 51.03 “Sexual Harassment, Sexual Assault, Sexual Misconduct, and Title IX Policy and Complaint Procedure” for additional information.

Users must not purposely engage in activities that may harass (including sexual harassment), threaten, or abuse others. This includes, but is not limited to:

1. Using email or messaging services to harass or intimidate another person.
2. Broadcasting unsolicited messages.
3. Sending unwanted email repeatedly.

5. 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. Offensive Websites

TTUHSC is not responsible for content that users may encounter while using the internet. If users connect to websites containing objectionable content, they must promptly move to another site or terminate their session. Furthermore, if it is discovered that a website contains sexually explicit, racist, sexist, violent, or other potentially offensive material, they must immediately disconnect from that site. Exceptions are made for material used for scientific, medical, or educational purposes.

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 malicious sites that are likely to cause network service degradation (e.g., graphics, video, and music files).

6. 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 specific approval of the IT Division.

7. 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. Sexually Explicit Material

1) Users must not intentionally access, create, store, or transmit material that TTUHSC may deem to be offensive, indecent, or obscene on IR. This includes both visual and textual sexually explicit material as defined by Chapter 43 of the State of Texas Penal Code on Public Indecency. Exceptions may be made for material used for scientific and medical research, patient care, or educational purposes.

2) Display of explicit or offensive calendars, posters, pictures, drawings, cartoons, screen savers, emails, internet, or other multi-media materials in any format that reflects disparagingly upon a class of persons or a particular person in a protected category may constitute unlawful harassment. See TTUHSC OP 51.02. Display of sexually explicit visual material (calendars, posters, cards, software, internet, or other multimedia materials) may also constitute unlawful sexual harassment or Sexual Misconduct under TTUHSC policies. See TTUHSC OP 51.03.

3) 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

4) 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.

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 transport software provided by TTUHSC to another computer site without prior authorization from the IT Division. To do so without authorization constitutes theft.

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

4) Users must not use unauthorized software listed in TTUHSC IT policy 56.15 “Hardware Standards, Authorized Software, and Unauthorized Software” 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 Checking

Externally supplied CD-ROMs, USB flash drives, and other removable storage media will be automatically checked for viruses when introduced to TTUHSC systems.

8. Personal Equipment

Use of personal laptops, desktops, and tablets are not allowed for the creation and storage of TTUHSC information. Only email should 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 the computer system to which they are connected or using contains sensitive information, users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

9. Unauthorized Use

a. Peer-to-Peer Programs

1) Use of all 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.

b. 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 IR.

c. 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.

d. Guest Wireless Network

Students, faculty, and staff may not connect their personal computers to the guest wireless network in order to complete TTUHSC business-related activities. Guest wireless internet access

has been established for non-TTUHSC devices; in addition, TTUHSC devices that connect to the guest network may be disconnected without notice by the ISO.

10. 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 IR is a violation of the policies contained herein and can result in disciplinary action in accordance with, but not limited to, TTUHSC OPs 70.31 "Employee Conduct, Coaching, Corrective Action, and Separation from Employment" and 77.05 "Suspension and Retention," as well as the Student Handbook.

Related Statutes, Policies, and Requirements

Digital Millennium Copyright Act
Digital Millennium Copyright Act of 1998

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

Payment Card Industry (PCI) Data Security Standard (DSS)
PCI-DSS: 12.3 Acceptable Usage

Texas Administrative Code
TAC 202, Subchapter C, 70-76

Texas Public Information Act
Texas Public Information Act

Texas Security Control Standards Catalog
Texas DIR Security Control Standards Catalog

TTUHSC IT Areas of Responsibility
Areas of Responsibility

IT Division Document Details

Approval and Ownership

Approved By	Chip Shaw
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