



TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, **Use of Information Technology Resources**

PURPOSE: The purpose of this Operating Policy and Procedure is to provide the policy requirements for the use of Information Technology (IT) resources and associated data within Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso). This policy outlines general compliance instructions, and responsibilities for the use of information technology resources. Detailed policy information is located at <https://el Paso.ttuhscc.edu/it/policies/>.

REVIEW: This Operating Policy and Procedure will be reviewed in February of each odd-numbered year (ONY) by the Chief Information Officer (CIO).

INTRODUCTION:

This policy governs the use of Information Technology (IT) resources by students, faculty, staff and authorized users within TTUHSC El Paso. A comprehensive set of IT policies and procedures is located at <https://el Paso.ttuhscc.edu/it/policies/>, which is adopted by reference in this operating policy and procedure.

POLICY/PROCEDURE:

A. Information Security Officer

The Information Security Officer, who is appointed by the agency head or his/her designated representative, is responsible for developing, implementing, and maintaining IT systems and policies regarding the security, privacy, and integrity of IT hardware, software, and data.

The Information Security Officer has authority to investigate inappropriate use of state property, which includes TTUHSC El Paso computers, videoconferencing systems, and network activity.

B. User Privacy/Investigations

1. Users of state property have no expectation of privacy for information created on or contained therein. TTUHSC El Paso has the right to disclose the contents of electronic files when required by legal purposes; audit purposes; or legitimate federal, state, local, or institutional purposes.
2. 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 El Paso personnel or TTUHSC El Paso computing facilities.

C. Approved Access Approval

Some jobs or activities of TTUHSC El Paso involve access to resources critical to computer security and privacy. TTUHSC El Paso may require that the authorized users involved in these jobs or activities submit to a background check, participate in special training, and/or sign special agreements concerning computer use.

D. Peer-to-Peer Programs

Use of all peer-to-peer programs (such as cloud and Dropbox) on TTUHSC El Paso computers and/or the TTUHSC El Paso network for the downloading and/or uploading of copies of copyrighted media is illegal and strictly prohibited.

Students, faculty, and staff may not use their personally owned computers to connect to the TTUHSC El Paso network. Guest Wireless has been provided for non-TTUHSC El Paso devices to use.

Non-TTUHSC El Paso devices that connect to a TTUHSC El Paso network that is not Guest wireless may be disconnected without notice by the ISO. If an employee must use VPN to connect remotely, they must first disable all peer-to-peer applications and services before connecting to the network. This includes direct connection or remote connection via PPP, VPN, or wireless accounts.

Any computers using peer-to-peer applications on the TTUHSC El Paso network are subject to removal from the network until the application is removed or disabled.

E. Disciplinary Repercussions

Misuse of TTUHSC El Paso IR is a violation of the policies contained herein and will result in disciplinary action in accordance with HSCEP OP's [70.31](#) and [77.05](#) as well as the Student Affairs Handbook.

F. Information Resources Acceptable Use Responsibility

IR at TTUHSC El Paso are owned by the State of Texas and administered by the IT Division. TTUHSC El Paso will provide access to appropriate resources to all members of the TTUHSC El Paso community. Users are responsible for managing their use of IR and are accountable for their actions relating to IT security.

G. Reporting Security Incidents

Users must report any weaknesses in TTUHSC El Paso computer security, any incidents of possible IR misuse, or any violation of IT policies. Employees should report incidents to their supervisor. Non-employees, including students, should report any incidents to the Information Security Officer (ISO).

Based upon the nature of the incident, appropriate actions to protect TTUHSC El Paso resources will be taken, and, if necessary, proper authorities will be contacted.¹

H. Authorized Access, Security Programs Authority

1. Users may use only the IR to which they have been given authorized access. Users must not attempt to access any data or programs for which they do not have authorization or explicit consent to access.²
2. A user must not download, install, or run security 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.³

Such programs include but are not limited to:

¹ TAC 202.73(A)&(B) and TTU OP 52.04(1)

² TAC 202.72(3)(a)&(b)

³ TAC 202.76

- a. Password cracking programs.
- b. Packet sniffers.
- c. Port scanners.
- d. Any non-approved programs on TTUHSC El Paso IR.

I. Keep Access Information Private

Users must not share their accounts, passwords, Personal Identification Numbers (PINs), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.⁴ Users who share their access with another individual will be responsible and held liable for all usage under their account.⁵

J. Copyright/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 El Paso to another computer site without prior authorization from the departmental administrator. To do so without authorization constitutes theft.
3. Users must not make unauthorized copies of copyrighted software.⁶
4. TTUHSC El Paso IR may not be used for illegally downloading any materials. This includes downloading materials through peer-to-peer (P2P) technology.
5. Users must not use software listed in the "unauthorized software list" without explicit approval of the Chief Information Officer (CIO) or the CIO's designee.⁷

K. Other

1. Do 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 El Paso network.
2. Do not install software/hardware for personal use on TTUHSC El Paso systems.

L. Sexually Explicit Material

1. Sexually explicit material in any form is not allowed on TTUHSC El Paso systems.
2. Users shall not view, retrieve, transmit, distribute, print, or save any electronic files that may be deemed sexually explicit on TTUHSC El Paso 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 are made for material used for scientific, medical, and/or educational purposes.

⁴ TAC 202.72(3)(b)

⁵ TAC 202.73(A)&(B)

⁶ Digital Millennium Copyright Act of 1998 and TTU OP 30.22

⁷ TAC 202.71(c)

3. It is also illegal to use sexually explicit material to intimidate, persecute, or otherwise harass another individual. This is considered sexual harassment. For more detailed guidelines on sexual harassment, refer to [HSCEP OP 70.14](#).
4. Do not open any emails which you believe to contain obscenity or pornography. If obscenity and/or pornography are 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 El Paso email address, report it to the Executive Director Human Resources and/or the Information Security Officer (ISO) immediately. The reporting of such a violation will be held in the strictest confidence.

M. Unreasonable Interference

Users must not unreasonably interfere with the fair use of IR by others. 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 El Paso network.

N. Further Prohibited Uses

1. Users are prohibited from using the TTUHSC El Paso systems or networks for personal or commercial gain. For example:
 - a. Selling access to your USER ID or to TTUHSC El Paso systems or networks.
 - b. Performing work for profit with TTUHSC El Paso resources in a manner not authorized by TTUHSC El Paso.
 - c. Marketing/advertising not authorized by the TTUHSC El Paso marketing/advertising Director.
 - d. Personal business transactions with commercial organizations.
2. TTUHSC El Paso systems are not to be used for partisan political purposes, such as using electronic mail to circulate advertising for political candidates or for the lobbying of public officials.

O. Harassment

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

1. Using mail or messaging services to harass or intimidate another person.
2. Broadcasting unsolicited messages.

3. Repeatedly sending unwanted mail.

P. Remote Access

Remote access to TTUHSC El Paso from any computer must comply with the same access policies that apply to use from within TTUHSC El Paso facilities.

Employees and students must not allow family members or other non-employees to access TTUHSC El Paso computer systems.⁸

Q. Incidental Use

TTUHSC El Paso IR are provided for the express purpose of conducting the business of TTUHSC El Paso. However, incidental use of IR is permitted as a convenience to the TTUHSC El Paso user community.

The following restrictions apply:

1. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on is restricted to approved users; it does not extend to family members or other acquaintances.
2. Incidental use must not result in direct or indirect costs to any TTUHSC El Paso institution.
3. Incidental use must not interfere with the normal performance of an employee's job duties.
4. 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 System.
5. Storage of personal email messages, voice messages, files, and documents within any institutional IR must be minimal and can be removed without notice or consent.
6. All messages, files, and documents- including personal messages, files, and documents- located on institutional IR are owned by the institution and may be subject to open records requests and may be accessed in accordance with this policy.⁹
7. Users of state-owned IR shall have no expectation of privacy except as otherwise provided by applicable privacy laws.

R. Conclusion

The above policy provides a basic framework for acceptable and unacceptable activities for IR usage.

All other IT Policies can be found at <https://el Paso.ttuhs c.edu/it/policies/>

⁸ TAC 202.72(3)(b)

⁹ Texas Public Information Act