TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

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

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to provide policy requirements for the use of Information Technology (IT) resources and associated data within TTUHSC El Paso. This policy outlines general compliance instructions and responsibilities for the use of IT resources. Detailed policy information and a comprehensive set of IT policies is located at the IT homepage under the policies link, which is adopted by reference in this HSCEP OP.

This policy governs the use of IT resources by students, faculty, staff and authorized users within TTUHSC El Paso.

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

POLICY/PROCEDURE:

I. General

A. Information Resources (IR) procured with TTUHSC El Paso funds are owned by the State of Texas and administered by the IT Department. 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 for official duties as permitted by this policy.

B. Users of state property and those working on behalf of the institution have no expectation of privacy regarding information created, sent, received, or stored on institution-owned computers, servers, or other IR owned by, or held on behalf of TTUHSC El Paso.

C. Users have no expectation of privacy for institutional data residing on personally owned devices, regardless of why the data was placed on the personal device. TTUHSC El Paso may monitor its IR without notice.

D. TTUHSC El Paso has the right to disclose the contents of electronic files when required for legal purposes; audit purposes; or legitimate federal, state, local, or institutional purposes.

E. Users of IR and personal devices are responsible for managing their use and are accountable for their actions relating to IT security policies and procedures and are required to comply with institutional IR use and security policies at all times.

F. TTUHSC El Paso may temporarily or permanently revoke access, privileges, and/or use of IR at any time for abusive conduct, policy violations, or security risks.

G. Use of IR to deprive access to individuals otherwise entitled to access institutional information, to interfere with the fair use of IR by others, to circumvent institutional computer security measures; or, in any way that is contrary to TTUHSC El Paso's mission(s) or applicable law is prohibited.

H. Incidental use of IR must not interfere with the normal performance of an employee's job duties.

I. Use of TTUHSC El Paso IR must be consistent with applicable laws and university policies.

J. Use of TTUHSC El Paso IR to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the user's official duties and is approved in writing by the president or a specific designee. Viewing, access to, storage or transmission of sexually explicit materials on IR as incidental use is prohibited.

K. All messages published as representative of TTUHSC El Paso must be approved by TTUHSC El Paso prior to public communication.

L. Users are required to report misuse of IR or violations of this policy to the TTUHSC El Paso information security officer (ISO).

M. All products and information created on Institutional property or while working as an Institutional representative on personal devices belong to the institution. These products shall be considered "intellectual property" as defined by the Board of Regents Rules and Regulations, Chapter 10-Intellectual Property Rights.

II. Privileged Users

A. All personnel with elevated privileges pose a higher risk to the institution than a standard user. As such, privileged users have greater responsibilities to ensure the secure operation of any TTUHSC El Paso system, and are held to a higher standard in regards to disciplinary action. All elevated privileges will be approved by the ISO and are subject to be removed at any time without notice.

B. Users are prohibited from using network scanning, sniffing, or hacking tools on the TTUHSC El Paso network. This includes the usage on personal devices as well as IR to store, transmit, or process information. All software installed must be approved by the IT Cybersecurity Office for usage on the TTUHSC El Paso network.

C. Users are prohibited from using programming tools on their IR or personal devices to run programs or scripts while in the TTUHSC El Paso networking environment. All usage of programming tools and associated software must be approved by the IT Cybersecurity Office.

III. Confidentiality and Security of Data

A. Users may use only the IR to which they have been given authorized access and only for the capacity to conduct official business for which the user is employed.

B. Users must not attempt to access any web sites, data, or programs for which they do not have authorization or explicit consent to access. Individuals should only access information that is their own, that is publicly available, or to which they have been given authorized access by TTUHSC El Paso.

C. Users must not disclose or share confidential information, except as required by law, authorized by official duties, and with formal agreements that ensure third parties will adequately protect it. Users are responsible for meeting all Federal, State, and local regulatory requirements.

D. Whenever feasible, users shall store Institutional confidential information or other

information essential to the mission of TTUHSC El Paso on a centrally managed server, rather than a local hard drive or portable device.

E. Users should not store confidential data on mobile devices without proper authorization; however, in cases when a user must create or store confidential or essential information on a portable device such as a laptop computer, tablet computer, or, smart phone, the user must ensure the data is encrypted in accordance with applicable information security data handling requirements. The same security requirements apply to storage on local hard drives as well.

F. Users must not transport, transfer, email, remotely access, or download non-public information, unless such action is explicitly permitted by TTUHSC El Paso, the manager or owner of such information.

G. Users are not authorized to use removable media drives such as USB or external hard drives without approval from the IT Cybersecurity Office. Under no circumstances shall unencrypted drives be used to store Institutional data without approval from the IT Cybersecurity Office.

H. Users are responsible for understanding TTUHSC El Paso data handling requirements, and ensuring their data handling and usage is in compliance at all times.

I. Email sent to and received from institutionally provided email accounts is automatically encrypted in transit when regulated data is detected. The IT Department will provide tools and processes for users to send encrypted data over unsecured networks to and from other locations.

J. Users must not intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.

K. Any computers on the TTUHSC El Paso network using unapproved peer-to-peer applications, malicious applications, or software that does not agree with the institution's mission and vision, are subject to removal from the network until the application is removed or disabled. Users are not authorized to install software not approved by the IT Department.

L. Students, faculty, and staff must use the guest wireless if they use their personally owned computers to connect to the TTUHSC El Paso network. TTUHSC El Paso devices that connect to the TTUHSC El Paso guest network may be disconnected without notice by the ISO.

M. All remote access to networks owned or managed by TTUHSC El Paso must be accomplished using a remote access method approved by the IT Cybersecurity Office and comply with IT security policies.

N. All computers connecting to a TTUHSC El Paso network remotely, must run security software approved by the ISO to properly secure IR.

O. Users who store institutional data using commercial cloud services must use only those services provided or sanctioned by TTUHSC El Paso, rather than personally obtained cloud services. Users must not establish any third-party information storage network that will handle TTUHSC El Paso information without the approval of the IT Department.

P. A user must not download, install, modify software 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.

Q. Users must not use security programs or utilities except those programs that are required to perform their official duties on behalf of institution, or those that information security requires to be installed in order to access the TTUHSC El Paso network and IR.

R. Devices lacking required security software or otherwise posing a threat to IR and the institution, may be immediately disconnected from the network without notice.

S. Intentionally running a program that attempts to violate the operational integrity of the TTUHSC El Paso network or intentionally circumvent or disrupt information security in any way is prohibited.

IV. Email

A. Use of organization-provided IT resources for personal commercial purposes, in support of "for-profit" activities or in support of other outside employment or business activity is prohibited.

B. Emails sent or received in the course of conducting institutional business are subject to state records retention and security requirements.

C. Users are to use institutional provided email accounts, rather than personal email accounts, for conducting official business.

D. The following email activities are prohibited when using an institutional provided email account:

1. Sending an email under another individual's name or email address,

2. Accessing the content of another user's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the user's official duties on behalf of TTUHSC El Paso.

3. Sending or forwarding any email that is unauthorized mass mailing or suspected by the user to contain computer viruses.

4. Forwarding your TTUHSC El Paso email to your personal email account, or creating rules to automatically forward emails to a personal account or cloud storage.

5. Copying or downloading of confidential or regulated institutional emails or files to a personal device using institutional email

E. Any non-business related usage of TTUHSC El Paso email prohibited by this policy.

V. Incidental Use of Information Resources

A. Incidental use of IR must not interfere with user's performance of official business, result in direct or indirect costs to TTUHSC El Paso, expose the institution to unnecessary risks, or violate applicable laws or other Institutional policy. Incidental usage is expected to be kept to a minimum.

B. Users must understand that they have no expectation of privacy in any personal information stored, transmitted, or created on an IR.

C. Incidental personal use of IR does not extend to a user's family members or other acquaintances regardless of physical location. Employees and students must not allow family members or other non-employees to access TTUHSC El Paso IR.

D. Incidental use to conduct or promote the user's outside employment, self-employment, outside fundraising, endorsing any product or service, for partisan political purpose, lobbying, or campaigning is prohibited.

E. Using IR to store personal email messages, voice messages, files, and documents may result in removal of the data without notice or consent.

F. 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 public information requests and may be accessed in accordance with this policy.

G. Files not related to Institutional business may not be stored on TTUHSC El Paso file servers or storage solutions.

VI. Portable and Remote Computing

A. Employees are not authorized to use personal computers, smart phones, or other devices to conduct institutional business involving confidential or regulated data. Physicians are only authorized to use personal devices for connection to designated systems that are properly secured for the use of personal devices. All other access is prohibited.

B. All electronic devices including personal computers, smart phones or other devices used to access, create or store IR must be password protected in accordance with information security requirements.

C. Institutional data created or stored on user's personal computers, smart phones or other devices, or in data bases that are not part of TTUHSC El Paso's IR are subject to Public information requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to institutional information resources.

D. Institution-owned mobile computing devices must be encrypted.

E. Any personally owned computing devices on which non-public institutional data is stored or created must be encrypted.

F. Institutional data created and/or stored on personal computers, other devices and/or non-institutional data bases should be transferred to institution-owned IR as soon as feasible.

G. Unattended portable computers, smart phones and other computing devices must be physically secured. Methods to secure IR include but are not limited to:

1. Logging off or locking systems when leaving them unattended,

2. A 15-minute timeframe is established for systems to obscure the contents of the computers when inactive,

3. Keeping sensitive information out of sight when visitors are present.

VII. Authentication Management

A. Passwords, including digital certificate passwords, Personal Identification Numbers (PIN), digital certificates, security tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. All authentication mechanisms must be approved by TTUHSC El Paso IT Security.

B. Each User is responsible for all activities conducted with the user's authentication credentials.

VIII. Disciplinary Repercussions/Sanctions

A. 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. Users of IR are also subject to 56.50 IT Sanctions policy (SN), for failure to adhere to IT Security policies and procedures.

All other IT Policies can be found at https://elpaso.ttuhsc.edu/it/policies/