TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.50 - Data Handling Guidelines

Policy Statement:

TTUHSC El Paso shall develop, document, implement, and periodically update measures to protect its critical systems and data.

Reason for Guidelines:

The purpose of the Data Handling Guidelines is to support Data Classification guidelines and assessing risk as it pertains to data collected, stored, maintained, and accessed at TTUHSC El Paso. Guidelines work in concert with IT security policies to comply with state and federal regulations that require the protection and security of data utilized, accessed, and/or housed by TTUHSC El Paso. It is a protocol to ensure due care and careful considerations given to minimize risks to TTUHSC El Paso.

Entities affected by this policy are any and all users of information resources at TTUHSC El Paso.

What is covered in this set of guidelines?

The overall guidelines address the institutional stance as it applies to TTUHSC El Paso in the areas of: data categorization, risk assessment categories, and best practices for data management.

It is the stance of TTUHSC El Paso to ensure that there are safeguards in place aligned with NIST 800-53 and TAC 202 to ensure the protection, integrity, and confidentiality of information resources at TTUHSC El Paso.

Who should read these guidelines?

All individuals accessing, storing, viewing any TTUHSC El Paso information resources.

What happens if I violate these guidelines?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under federal, state, and local legislation. Attestation and data security are a professional expectation and personal responsibility at TTUHSC El Paso; failure or interference to comply with and/or correctly encrypt and protect all data and devices according to state and federal guidelines will result in remediation efforts as outlined in HSCEP OP 56.50 Sanctions Policy.1

Review

These guidelines will be reviewed and updated March of every odd-numbered year (ONY) by the Information Security Officer (ISO) and the Chief Information Officer (CIO).

Policy

Data owners/custodians are responsible for any information disclosure from your computer or mobile devices, whether accidental or not.

For every end user accessing protected data, every device used to access TTUHSC El Paso information resources, network, and/or data, must be verifiably encrypted. If you have a device that cannot meet the encryption requirements, it must not be used for TTUHSC El Paso work. This applies to both TTUHSC El Paso owned as well as personally-owned devices.

Guidelines

The following table lists the types of information that is recommended according to NIST

data handling guidelines.

Handling Controls	Restricted/Regulated	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-TTUHSC El Paso employees.	▪ NDA is recommended prior to access by non-TTUHSC El Paso employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark “Open by Addressee Only” ▪ Use “Certified Mail” and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer	▪ Verify destination printer	▪ Verify destination printer	*No special requirements*

	▪ Attend printer while printing	▪ Attend printer while printing	▪ Retrieve printed material without delay	
Web Sites	▪ Posting to intranet sites is prohibited unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is prohibited unless it is pre-approved to contain Restricted data.	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*
Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*
Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

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

1. 56.50 Sanctions Policy (SN)
2. NIST 800-53 A-5 Data Handling Guidelines

Revised: January 2018