TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.50 - Data Classification 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 Classification Guidelines is 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 policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of data categorization, best practices, and data management.

Who should read these guidelines?

All individuals accessing, storing, or 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 to comply or interference with correctly encrypting and protecting 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 by the Information Security Officer (ISO) and the Chief Information Officer (CIO).

Guidelines statement

You are responsible for any information disclosure from your computer or mobile devices, whether accidental or not. For every end user accessing this type of 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.

Policy

You are responsible for any information disclosure from your computer or mobile devices, whether accidental or not.

For every end user accessing this type of 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.

Information Owners are required to:

- Classify information under their authority, with the concurrence of the state institution of higher education head or his or her designated representative(s), in accordance with the institution of higher education's established information classification categories;
- Formally assign custody of information or an information resource; coordinate data security control requirements with the ISO;
- Convey data security control requirements to custodians;
- Provide authority to custodians to implement security controls and procedures;
- Justify, document, and account for exceptions to security controls that have been coordinated and approved according to security controls with TTUHSC El Paso's Information Security Officer.

Data Custodians are required to:

- Implement controls required to protect information and information resources required by this chapter based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the institution of higher education information security program;
- Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.

User Responsibilities require the user of an information resource to:

- Use the resource only for the purpose specified by the institution or information-owner;
- Comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
- Formally acknowledge that they will comply with the security policies and procedures in a method determined by the institution head or his or her designated representative

Guidelines

Data encryption

- Social Security Number (SSN)/Taxpayer Identification Number (TIN)/National Identification Number (NIN)
- Passport Number
- Permanent resident card
- Driver's License (DL)
- Financial account number (credit or debit)
- Bank account number
- Electronic Protected Health Information (ePHI)
- FERPA Information
- HIPAA Information
- Health Insurance policy ID numbers
- Export controlled information under U.S. Laws
- Donor contact information and non-public gift information
- Data Classification
- Assumptions of Data Classification:

Data Classification

Assumption of Data Classification:

- Any information created or received by TTUHSC El Paso employees in the performance of their jobs is at Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential Information, the entire application is confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels

Classification	Data Classification Description	
Restricted/Regulated	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	**SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to TTUHSC El Paso.
		Impact could include negatively affecting TTUHSC El Paso’s competitive position, violating regulatory requirements, damaging the company’s reputation, violating contractual requirements, and posing an identity theft risk.
Confidential	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by TTUHSC El Paso.
	Potential Impact of Loss	**MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to TTUHSC El Paso.
		Impact could include negatively affecting TTUHSC El Paso’s competitive position, damaging the company’s reputation, violating contractual requirements, and exposing the geographic location of individuals.
Internal Use	Definition	Internal Use information is information originated or owned by TTUHSC El Paso, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company’s business interests.

	Potential Impact of Loss	**MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to TTUHSC El Paso.
		Impact could include damaging the company’s reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	**NO DAMAGE** would occur if Public information were to become available to parties either internal or external to TTUHSC El Paso.
		Impact would not be damaging or a risk to business operations.

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