HSCEP OP: 56.50 – Personnel Security (PS)

Policy Statement:

TTUHSC El Paso shall ensure that published rules of behavior are followed by users and employ a method of formal sanctions for personnel who fail to comply with IT security policies and standards.

Reason for Policy:

The purpose of the Personnel Security (PS) policy is to ensure that TTUHSC El Paso performs due are and due diligence in its personnel management of procedures.

Entities Affected by this Policy are any and all users of Information Resources at TTUHSC El Paso.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of: personnel security policy & procedures, position risk designation, users with elevated privileges, security-related positions, personnel screening, information with special protection measures, personnel termination, asset collection, high-risk terminations, personnel transfer, access agreements, third-party personnel security, personnel sanctions, and workplace investigations.

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 this Policy?

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

What happens if I violate this policy?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under federal, state, and local legislation. Disciplinary actions are further outlined in HSCEP OP 56.50, Sanctions Policy.

PS-01: Personnel Security Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:2

- A formal, documented security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

TTUHSC El Paso is required to document organization-wide personnel security controls that, at a minimum, include:

a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PS-02: Position Risk Designation (Position Categorization)

TTUHSC El Paso:

- Assigns a risk designation to all positions;
- Establishes screening criteria for individuals filling those positions; and
- Reviews and revises position risk designations.

TTUHSC El Paso's IT security personnel are responsible for assigning risk to job positions. Assigned risk is required to:

- Be consistent with HR policy and guidance;
- Include explicit information security role appointment requirements (e.g., training, responsibilities, etc.); and
- Prevent personnel who do not have access to sensitive data from obtaining access to sensitive data.

Risk Categorization Includes:

Users With Elevated Privileges
TTUHSC El Paso ensures that every user accessing a system processing, storing, or transmitting classified information is cleared and indoctrinated to the highest classification level of the information on the system. TTUHSC El Paso is required to diligently manage individuals with elevated privileges through the following methods:

a. Privileged access must be based on a legitimate need to have system access (e.g., "need to know" or "need to use"), and be re-evaluated annually;
b. Users with privileged access must be provided with periodic security awareness briefings and trained to fulfill their security responsibilities; and
c. A process to ensure access privileges are revoked in a timely manner when the requirement for access ceases (e.g., transfer, resignation, retirement, change of job description, etc.) and immediately for individuals being separated for adverse reasons just prior to notifying them of the pending action.

Security-Related Positions
The organization ensures that all security-related positions are staffed by qualified individuals and those individuals have the skill set necessary to perform the information security-related job functions. TTUHSC El Paso is required to assess individual skill sets for all individuals that are responsible for information security functions. Only individuals meeting or exceeding TTUHSC El Paso's information security skills requirement are allowed to perform information security-related functions.

PS-03: Personnel Screening

TTUHSC El Paso:

- Screens individuals prior to authorizing access to the system; and
- Rescreens individuals, if necessary, based on organizational concerns.

Human Resources (HR) is responsible for screening potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources.

Personnel Screening Includes:

Information With Special Protection Measures
TTUHSC El Paso ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

- Have valid access authorizations that are demonstrated by assigned official government duties; and
- Satisfy organization-defined additional personnel screening criteria.

TTUHSC El Paso management is required to ensure authorized users meet personnel screening criteria.

PS-04: Personnel Termination

TTUHSC El Paso, upon termination of individual employment:

- Terminates system access;
- Conducts exit interviews;
- Retrieves all security-related organizational system-related property; and
- Retains access to organizational information and systems formerly controlled by the terminated individual.

TTUHSC El Paso is required to ensure that upon termination of an individual's employment:

- System accounts are disabled with twenty-four (24) hours of the termination action;
- Exit interviews are conducted, if possible;
- All company-related property is recovered; and
- All company-owned information the terminated employee was responsible for is identified and accounted for.

Personnel Termination Includes:

Asset Collection
TTUHSC El Paso, upon termination of individual employment, ensures for the collection of organization-owned assets prior to the individual's departure. The direct manager of a terminated user is responsible for inventorying and accounting for all TTUHSC El Paso-issued assets, prior to the individual's departure.

High-Risk Terminations
TTUHSC El Paso, upon termination of an individual deemed to be "high-risk" to the organization, ensures for the expedited process of removing the individual's access to organizational systems and data. Human Resources (HR) is required to immediately notify TTUHSC El Paso's IT security personnel to revoke the user's IDs, privileges, and authorizations for a "high-risk" employee or contractor termination.

PS-05: Personnel Transfer

TTUHSC El Paso reviews logical and physical access authorizations to systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within an organization-defined time period following the formal transfer action:6

TTUHSC El Paso managers are required to:

- Review the logical and physical access authorizations to systems/facilities when personnel are reassigned or transferred to other positions within the company; and
- Initiate company-defined transfer or reassignment actions within seven (7) days following the formal transfer action.

PS-06: Access Agreements

TTUHSC El Paso:

- Ensures that individuals requiring access to organizational information and systems sign appropriate access agreements prior to being granted access; and
- Reviews/updates the access agreements.

TTUHSC El Paso is required to ensure that access to information with special protection measures is granted only to individuals who:

a. Have a valid access authorization; and

b. Satisfy associated personnel security criteria

PS-07: Third-Party Personnel Security

TTUHSC El Paso:

- Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- Document personnel security requirements; and
- Monitors provider compliance.

TTUHSC El Paso is required to ensure third-party personnel access is granted only to individuals who:

a. Have a valid access authorization;
b. Satisfy associated personnel security criteria;
c. Have read, understand, and signed a Non-Disclosure Agreement (NDA); and
d. Have read, understand, and signed an acknowledgment that he or she understands and will abide by TTUHSC El Paso's policies, procedures, standards, and guidelines.

PS-08: Personnel Sanctions

TTUHSC El Paso employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

TTUHSC El Paso HR is required to manage and operate its personnel sanctions process consistent with applicable laws, regulations, policies and standards.

Personnel Screening Includes:

Workplace Investigations

TTUHSC El Paso establishes guidelines for employee misconduct investigations.

TTUHSC El Paso is required to follow established guidelines for employee misconduct investigations:

a. All applicable laws concerning misconduct investigations will be adhered to;
b. Employees who become the subject of an internal investigation will be treated with dignity and respect, and will be provided with timely information about the outcome of the investigation, although TTUHSC El Paso reserves the right to restrict access to the investigation report and related documentation; and
c. Communications and work products relative to an investigation will be limited to parties with a legitimate need to know.

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

56.50, Sanctions Policy (SN)
NIST CSF PR.IP-11
HIPAA 164.308(a)(i) & (ii) &(A) | NIST CSF PR.IP-11 | PCS DSS 12.4 & 12.4.1
HIPAA 164.308(a)(3)(ii) & (B) | PCI DSS 12.7 | NIST CSF PR. DS-5 & PR.IP-11
HIPAA 164.309(a)(ii) & (C) | PCS DSS 9.3 | MA201CMR17 17.03(2)(e) | NIST CSF PR.IP-11
NIST CSF PR.IP-11
HIPAA 164.308(a)(4)(i) | NIST CSF PR.DS-5 & PR.IP-11
NIST CSF ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11
HIPAA 164.308(a)(1)(ii)(C) | MA201CMR17 17.03(2)(d) | NIST CSF PR. IP-11
Fair & Accurate Credit Transaction Act (FACTA) | Fair Credit Reporting Act (FCRA)

Revised May 2018