TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.50 - Program Management (PM)

Policy Statement:

TTUHSC El Paso shall implement IT security program management controls to provide a foundation for TTUHSC El Paso's Information Security Management System (ISMS).

Reason for Policy:

The purpose of the Program Management (PM) policy is for TTUHSC El Paso to specify the development, implementation, assessment, authorization, and monitoring of the IT security program management. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization's program management controls. The IT security Program Management (PM) controls are essential for managing the IT security program.

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 allocation of resources, system development lifecycle, acquisition process, access restriction for change, software usage restrictions, user-installed software, security engineering principles, external information system services, developer configuration management, and developer security testing.

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.

PM-01: Information Security Program Plan
TTUHSC El Paso:

- Develops and disseminates organization-wide information security standards that:
  - Provides an overview of the requirements for the information security program and a description of the controls in place, or planned, for meeting those requirements;
  - Provides sufficient information about controls to enable an implementation that is unambiguously compliant with the intent of the plan;
  - Includes roles, responsibilities, management commitment, and compliance;
  - Is approved by senior management with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations;
- Reviews standards for applicability; and
- Revises standards to address organizational changes and problems identified during implementation or

security assessments.
- Creates an information security program that is required to be approved by the chief information officer (CIO) on an annual basis.

TTUHSC El Paso's information security policies and standards shall be represented in a single document, the Written Information Security Program (WISP) that shall be:

- Endorsed by executive management;
- Reviewed and updated at least annually; and
- Disseminated to the appropriate parties to ensure all TTUHSC El Paso personnel understand their applicable requirements.

PM-02: Assigned Information Security Responsibilities

TTUHSC El Paso appoints an individual assigned with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

The authority and responsibility for managing the information security program are delegated to TTUHSC El Paso's Information Security Officer (ISO and he/she is required to perform or delegate the following information security management responsibilities:

- Establish, document, and distribute security policies and procedures;
- Monitor and analyze security alerts and information;
- Distribute and escalate security alerts to appropriate personnel;
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
- Administer user accounts, including additions, deletions, and modifications; and
- Monitor and control all access to data.

PM-03: Information Security Resources

TTUHSC El Paso addresses all capital planning and investment requests, including the resources needed to implement the information security program, and documents all exceptions to this requirement.

The Information Security Officer (ISO) and his/her designated representatives are responsible for managing and providing oversight for the information security-related aspects of the planning and service/tool selection process.

PM-04: Vulnerability Remediation Process

TTUHSC El Paso implements a process for ensuring that vulnerabilities are properly identified, documents remediation actions and tracks vulnerabilities to mitigate risk to operations, assets, individuals, and other organizations.

TTUHSC El Paso is required to use a Plan of Action & Milestones (POA&M), or some other company-approved method, as a key tool in documenting identified weaknesses, their status, and remediation steps.

PM-05: Information System Inventory

TTHUSC El Paso develops and maintains an inventory of its systems.

TTUHSC El Paso is required to maintain an inventory of its systems that includes, but is not limited to:

a. A list of all such devices and personnel with access;
b. A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices);
c. List of company-approved products; and
d. Update the inventory at necessary.

PM-06: Information Security Measures of Performance

The organization develops, monitors, and reports on the results of information security measures of performance.

The Information Security Officer (ISO) is responsible for developing measures of performance or outcome-based metrics to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

PM-07: Enterprise Architecture

TTUHSC El Paso develops an enterprise architecture, aligned with industry-recognized leading practices, with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations.

TTUHSC El Paso's enterprise architecture process shall be:

a. Aligned with the industry-recognized leading practices; and
b. Utilized in all system development and acquisition activities.

Enterprise Architecture includes:

Standardized Terminology
TTUHSC El Paso uses standardized terminology to reduce confusion amongst groups and departments.

TTUHSC El Paso shall use the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, Glossary of Key Information Security Terms, as the primary reference document to define common information security terms.

PM-08: Statutory, regulatory & Contractual Compliance

TTUHSC El Paso addresses information security issues in the development, documentation, implementation, and updating of a plan to protect its critical systems and sensitive data in accordance with applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound to address.

Asset custodians and data/process owners are required to protect TTUHSC El Paso's critical systems and sensitive data in accordance with applicable US local, state, and Federal laws, as well as applicable international and other legal requirements that TTUHSC El Paso is contractually bound to address.

PM-09: Risk Management Strategy

TTUHSC El Paso:

- Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations associated with the operation and use of systems; and
- Implements that strategy consistently across the organization.

TTUHSC El Paso is required to use an organization-wide information security risk management strategy that includes;

a. A formal risk assessment that is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
b. Identification of critical assets, current safeguards, effectiveness of safeguards, threats, and vulnerabilities;
c. A review of all processes involving creating, receiving, maintaining and transmitting of sensitive data; and
d. Assigning responsibility to validate security controls are enabled.

PM-10: Security Authorization Process

TTUHSC El Paso:

- Manages the security state of organizational systems through security authorization processes;
- Designates individuals to fulfill specific roles and responsibilities within the organization's risk management process; and
- Fully integrates the security authorization processes into an organization-wide risk management program.

The Information Security Officer (ISO) and his/her designated representatives are responsible for managing the state of TTUHSC El Paso's information security infrastructure.

PM-11: Business Process Definition

TTUHSC El Paso:

- Defines business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations; and
- Determines information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Managers are required to work with asset custodians and data/process owners to formally document the established businesses processes to ensure that security considerations are addressed early in the System Development Life Cycle (SDLC), in order to integrate information security requirements and associated security controls into the enterprise architecture.

PM-12: Insider Threat Program

TTUHSC El Paso organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

The Information Security Officer (ISO) and his/her designated representatives are responsible for developing and implementing an insider threat program.

PM-13: Information Security Workforce

TTUHSC El Paso establishes an information security workforce development and improvement program.

The Information Security Officer (ISO) and his/her designated representatives are responsible for developing and implementing an information security workforce development and improvement program.

PM-14: Testing, Training & Monitoring

TTUHSC El Paso:

- Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems;
  - Are developed and maintained; and
  - Continue to be executed in a timely manner;
- Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

The Information Security Officer (ISO) and his/her designated representatives are responsible for establishing and maintaining a process to:

a. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:
   i. Daily log reviews;
   ii. Firewall ruleset reviews;
   iii. Applying configuration standards to new systems;
   iv. Responding to security alerts; and

    v. Change management processes;
  b. Maintain documentation of quarterly review process to include:
    i. Documenting results of the reviews; and
    ii. Review and sign-off of results by personnel assigned responsibility for the compliance program.

PM-15: Contacts With Security Groups & Associations

TTUHSC El Paso establishes and institutionalizes contact with selected groups and associations within the security community to:

- Facilitate ongoing security education and training for organizational personnel;
- Maintain currency with recommended security practices, techniques, and technologies; and
- Share current security-related information including threats, vulnerabilities, and incidents.

The Information Security Officer (ISO) and his/her designated representatives are responsible for establishing and maintaining formal contact with selected groups and/or associations within the security community.

PM-16: Threat Awareness Program

TTUHSC El Paso implements a threat awareness program that includes a cross-organization information-sharing capability.

The Information Security Officer (ISO) and his/her designated representatives are responsible for establishing and implementing a formal threat awareness program to make all personnel aware of the importance of information security.

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

56.50, Sanctions Policy (SN)
HIPAA 164.308(a)(1) & 164.316(a)-(b) | GLBA Sec 6801(b)(a) | PCI DSS 12.1 & 12.1.1 | MA201CMR17 17.03(1), 17.04 & 17.03(2)(b)(b) |NIST CSF ID.GV-1 & ID.GV-2 | DFARS 252.204-7008
HIPAA 164.308(a)(2) | GLBA Safeguards Rule | PCI DSS 12.5-12.5.5 | MA201CMR17 17.03(2)(a) | OR646A.622(2)(d)(A)(i) | NIST CSF ID.AM-6 & ID.GV-2
MA201CMR17 17.03(2)(j) | OR646A.622(2)(d)(B)(iii) | NIST CSF ID.RA-6
PCI DSS 12.3.3, 12.3.4 & 12.3.7 | NIST CSF ID.AM-1 & ID.AM-2
HIPAA 164.308(a)(8) | SOX Sec 404 | MA201CMR17 17.03(2)(j) | OR646A.622(2)(d)(A)(vi) & OR646A.622(2)(d)(B)(iii) | NIST CSF ID.AM-2 & PR.IP-7
PCI DSS 2.2
NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
HIPAA 164.308(a)(8) | GLBA Sec 6801(b)(c) | PCI DSS 12.1/NV SB 227 | NIST CSF ID.BE-2, ID.BE-4, ID.GV-3 & ID.RM-3
HIPAA 164.308(a)(1)(ii)(B) | SOX Sec 404 | GLBA Sec 6801(b)(b) | PCI DSS 12.1 | MA201CMR17 17.03(2)(b) | OR646A.622(2)(d)(A)(ii) | NIST CSF ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-6, ID.RM-1, ID.RM-2 & ID. RM-3
NIST CSF ID.AM-6, ID.BE-3, ID.GV-4, ID.RA-4, RA-4 & ID.RM-3
NIST CSF ID.RA-3
NIST CSF PR.AT-1, PR.AT-2, PR.AT-4 & PR.AT-5
NIST CSF PR.IP-1-, DE.DP-1, DE.DP-2, DE.DP-3 & DE.DP-5 | PCI DSS 12.11 & 12.11.1
HIPAA 164.308(a)(5)(ii)(A) | PCI DSS 5.1.2 & 6.1 | NIST CSF ID.RA-2 & RS.CO-5
PCI DSS 12.6 | NIST CSF ID.RA-2, ID.RA-3 & ID.RA-5
TAC §202.74

Revised May 2018