HSCEP OP: 56.50 - Planning (PL)

Policy Statement:

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

Reason for Policy:

The purpose of the Planning (PL) policy is to ensure due care planning considerations are addressed 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 Policy?

The overall policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of: security planning policy & procedures, system security plan (SSP), Security Plan Update, Rules of Behavior, Privacy Impact Assessment (PIA), Security-related Activity Planning, Concept of Operations, Security Architecture, and Central 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 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.

PL-01: Physical & Environmental Protection Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

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

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

a. A formal, documented security planning policy; and
b. Processes to facilitate the implementation of the security planning policy, procedures and associated controls.

PL-02: System Security Plan (SSP)

TTUHSC El Paso develops a functional architecture for identifying and maintaining key architectural information on each critical system that, at a minimum, includes:

- External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
- User roles and the access privileges assigned to each role;
- Unique security requirements;
- Types of information processed, stored, or transmitted by systems and any specific protection needs in accordance with applicable local, state and Federal laws; and
- Restoration priority of information or system services.

Asset custodians and data/process owners are required to document key architectural information on each critical system that, at a minimum, includes:

a. External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
b. User roles and the access privileges assigned to each role;
c. Unique security requirements;
d. Types of information processed, stored, or transmitted by systems and any specific protection needs in accordance with applicable local, state and Federal laws;
e. Restoration priority of information or system services; and
f. Reviewing and revising the security of their system(s) on an annual basis, or as otherwise necessary. The review process should consider, but not limited to, the following activities;
    i. Scope, impact, and urgency of any new threat(s) to TTUHSC El Paso;
    ii. Upcoming business initiatives and their potential security risk(s);
    iii. Mergers or acquisitions that have occurred and their potential security risk(s);
    iv. New technologies that have been introduced to TTUHSC El Paso's computing environment;
    v. Anticipated technologies that may be introduced into TTUHSC El Paso's computing environment;
    vi. Planned system conversions; and
    vii. Industry trends and recent releases of industry-recognized leading practice controls and benchmarks.

System Security Plan Includes:

Plan/Coordinate With Other Organizational Entities
Asset and process owners must plan and coordinate security-related activities affecting the information system potentially affected parties before conducting such activities in order to reduce the impact on other business operations.

Adequate Security For Covered Defense Information (CDI)
TTUHSC El Paso shall provide adequate security for all Covered Defense Information (CDI) on all covered contractor information systems that support the performance of work under any DoD contract. In terms of CDI, "adequate security" means that TTUHSC El Paso shall:

a. Implement information systems security protections on all Covered Contractor Information Systems (CCIS) including, at a minimum:
    i. For CCIS that are part of an Information Technology (IT) service or system operated on behalf of the Government-
        1. Cloud computing services are subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services; and
        2. Any other such IT service or system (i.e., other than cloud computing) are subject to the security requirements specified elsewhere in the DoD contract; or
    ii. For CCIS that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified DFARS 252.204-7012:
        1. The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017; or

2. Alternative, but equally effective, security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD; and

b. Apply other information systems security measures when TTUHSC El Paso reasonably determines that information systems security measures, in addition to those identified in DFARS 252.204-7012, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability

PL-04: Rules Of Behavior

TTUHSC El Paso:

- Develops usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email usage and Internet usage) and define proper use of these technologies.
- Verifies that the usage policies require acceptable uses for the technology.
- Verified that the usage policies require acceptable network locations for the technology.
- Prohibits copy, move, and storage of sensitive data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need; and
- Establishes end-user messaging technologies restrictions.

Information Security is responsible for developing usage policies for technologies and defining proper use of TTUHSC El Paso's technologies, ensuring:

- Systems can only be used after explicit approval is given by company management;
- User authentication must be enabled, when technically feasible;
- Acceptable uses of the technologies must be given; and
- Acceptable network locations must be clearly stated.

Rules Of Behavior Includes:

Social Media & Social Networking Restrictions
TTUHSC El Paso includes in the rules of behavior explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing system account information.

PE-08: Security Architecture

TTUHSC El Paso develops an information security architecture for systems that:

- Describes the overall philosophy and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; and
- Describes how the security architecture is integrated into and supports the enterprise architecture.

TTUHSC El Paso is responsible for developing and implementing a security architecture process.

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

56.50 Sanctions Policy (SN)
NIST CSF ID.AM-3
NIST CSF PR.IP-7 & DE.DP-5 | MA201CMR17 17.03(2)(b)(i)
DFARS 252.204-7012
HIPAA 164.310(b) | PCI DSS 4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-.6, 12.3.10 & 12.4 | MA201CMR17 17.03(2)(b)(b)
NIST CSF ID.RA-4
NIST CSF ID.AM-3 & PR.IP-2
TAC §202.74, §202.75

Revised May 2018