



## TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

### Operating Policy and Procedure

**HSCEP OP:** 56.50 – Awareness & Training (AT)

#### **Policy Statement:**

TTUHSC El Paso shall ensure that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards, and procedures related to the security of systems and data.

#### **Reason for Policy:**

The purpose of the Awareness & Training (AT) policy is to provide guidance for broad security awareness and security training for TTUHSC El Paso users. Security Awareness and training on information security protocols is essential for employees and students to minimize the likelihood of exposure to security breaches and to comply with state and federal law

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 Awareness Policy and procedures, training for sensitive information, vendor security training, training records, and industry alerts & notification processes.

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.

The Information Security Officer (ISO) is responsible for the selection, approval, and monitoring of security training materials and activities provided to and utilized by staff, faculty, and students.

#### **Who Should Read this Policy?**

Institutional IT security awareness training will be required for all staff, faculty, and students who access the TTUHSC El Paso network and/or data. This includes 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.

### **AT-01: Security Awareness and Training Policy and Procedures**

TTUHSC El Paso Information Security develops, disseminates, reviews & updates:

- A formal, documented security awareness and training 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 security awareness and training policy and associated security awareness and training controls.

TTUHSC El Paso is required to document organization-wide awareness and training controls that, at a minimum, include:

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

Basic Security Awareness and Training will be provided on an annual basis and will be delivered through the medium selected by Information Security

### **AT-02: Security Awareness**

TUHSC at El Paso provides basic security awareness training to all system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and thereafter as required[1]

TTUHSC El Paso's IT security personnel are responsible for developing and implementing a formal security awareness program to make all TTUHSC El Paso users aware of the importance of information security.

Security Awareness Includes:

#### **Practical Exercises**

TTUHSC El Paso's IT security personnel are responsible for developing and implementing practical exercises in security awareness training that simulate actual cyber-attacks.

#### **Insider Threat**

TTUHSC El Paso's IT security personnel are required to implement security awareness training that includes how to identify and report potential indicators of insider threat.

### **AT-03: Security Training**

TTUHSC El Paso provides role-based security-related training:2

- Before authorizing access to the system or performing assigned duties;
- When required by system changes; and
- Annually thereafter.

For Security Training:

- a. Human Resources (HR) and users' direct management shall provide initial security training to personnel upon hire; and
- b. TTUHSC El Paso's IT security personnel shall provide initial security training, and at least annually thereafter.

Security Training Includes:

#### **Awareness Training For Sensitive Information**

TTUHSC El Paso's management is required to ensure that every user accessing a system that processes, stores, or transmits sensitive information is formally trained in handling procedures for all of the relevant types of sensitive information.3

#### **Vendor Security Training**

TTUHSC El Paso is required to incorporate relevant security training to all employees and/or contractors that are involved in the deployment of information security-oriented solutions.

### **AT-04: Security Training Records**

TTUHSC El Paso:4

- Documents and monitors individual system security training activities including basic security awareness training and specific system security training; and
- Retains individual training records.

TTUHSC El Paso requires personnel to acknowledge in writing or electronically, at least annually, that they have read and understood TTUHSC El Paso's information security policies.

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

1. HIPAA 164.308(a)(5)(i) & 164.308(a)(5)(ii)(A) | PCI DSS 12.6 | MA201CMR17 17.04(8) & 17.03(2)(b)(a) | NIST CSF PR.AT-1
2. PCI DSS 12.6.1 | MA201CMR17 17.04(8) | OR646A.622(2)(d)(A)(iv) | NIST CSF PR.AT-2, PR.AT-4 & PR.AT-5
3. PCI DSS 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6, 12.6, 12.6.1, 12.6.2, 12.8.3 & 12.8.5, 12.10.4
4. PCI DSS 12.6.2
5. HIPAA 164.308(a)(5)(ii) & (ii)(A) | PCI DSS 6.2
6. 56.50 Sanctions Policy
7. TAC §202.74, §202.75
8. TAC §202.74
9. 45 CFR § 164.308 (5)(i)
10. TGC 2054.122
11. TAC 202 Control Catalog AT-1
12. TAC 202 Control Catalog AT-2
13. PCI DSS v3.2 - Sec 12.6
14. Computer Security Act of 1987 – Public Law 100-235 (H.R. 145) - Sec. 5
15. TAC §202.71
16. 45 CFR §164.308 (5)(ii)(A)
17. TAC 202 Control Catalog AT-3

*Revised: February 2018*