**HSCEP OP:** 56.50 – Certification, Accreditation & Security Assessment (CA)

**Policy Statement:**

TTUHSC El Paso shall periodically assess systems to determine if IT security controls are effective and ensure IT security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

**Reason for Policy:**

The purpose of the Certification, Accreditation & Security Assessment (CA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to the 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 security assessment policy & procedures, information system connections, security verification, plan of action milestones, security authorization, continuous monitoring, penetration testing, and internal system connections.

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.

# CA-01: Security Assessment Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates;

- Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, and compliance; and
- Processes to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

TTUHSC El Paso is required to document information security assessment controls that, at a minimum, include:

a. A formal, documented information security assessment procedure;
b. Processes to facilitate the implementation of information security assessments; and
c. Compliance with CIS Level 1 baselines/configuration standards.

# CA-02: Security Assessments

TTUHSC El Paso

- A qualified individual appointed by the ISO, independent of Information Security, assesses the security controls in systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
- Produces a security assessment report that documents the results of the assessment; and
- Provides the results of the security control assessment, in writing, to the senior information official or officially designated representative.

A formal information security risk analysis must be performed on all significant development and/or acquisitions, prior to systems being placed into production:

a. New systems and applications must be appropriately tested for functionality prior to being placed in production; and
b. Asset custodians and data/process owners are required to perform a gap analysis, at least once per year, to determine any deviations from their systems' current state of compliance and that which is required.

Security Assessments Include:

**Independent Assessors**
Whenever feasible, TTUHSC El Paso shall utilize independent assessors for security assessment functions.

**Specialized Assessments**
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall utilize specialized assessments to address unique areas of risk.

**External Organizations**
TTUHSC El Paso shall accept the findings of assessments, when performed by impartial, external organizations with subject matter expertise in the area being assessed.

## CA-03: Information System Connections

TTUHSC El Paso allows connections only from authorized systems to connect to the Local Area Network (LAN).

Only devices that are owned or managed by TTUHSC El Paso and meet CIS Level 1 baseline hardening standards are allowed to connect directly to TTUHSC El Paso's internal network(s).

Information System Connections Include:

**Unclassified Non-National Security System Connections**
TTUHSC El Paso prohibits the direct connection of a sensitive system to an external network without the use of an organization-definition boundary protection device.

**Restrictions On External System Connections**
TTUHSC El Paso prohibits the direct connection of a system to an external network without the use of a boundary firewall device.

**Demilitarized Zones**
If required for business needs, TTUHSC El Paso will:

- Implement a Demilitarized Zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
- Limit inbound Internet traffic to IP addresses within the DMZ; and
- Block internal addresses from passing from the Internet into the DMZ.

TTUHSC El Paso's IT department is require to implement and configure DMZs in accordance with

industry-recognized leading practices.

**Guest Networks**
If required for business needs, TTUHSC El Paso will implement a secure guest network.

Guest access is required to:

a. Be limited to a separate network that is logically separated;
b. Permit only authorized traffic between the guest environment and internal networks; and
c. Prevent direct access to TTUHSC El Paso's internal network(s).

## CA-04: Security Verification

TTUHSC El Paso:

- Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
- Monitors system connections on an ongoing basis verifying enforcement of security requirements.

Asset custodians and data/process owners are required to document the environment related to their systems which includes:

a. Description of business requirements for each interface connections;
b. Required security requirements; and
c. The data classification of the information communicated through the interface(s).

## CA-05: Plan Of Action & Milestones (POA&M)

TTUHSC El Paso:

- Develops a Plan of Action and Milestones (POA&M) for systems to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
- Update existing POA&M based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

In a Plan of Action & Milestones (POA&M), or some other TTUHSC El Paso-approved method, asset custodians and data/process owners are required to document:

a. All known vulnerabilities associated with the system(s);
b. Planned remedial actions to correct the identified weaknesses or deficiencies; and
c. Timeline to complete the remediation steps.

## CA-06: Security Authorization

TTUHSC El Paso:

- Assigns an Information Security Officer to the role of authorizing official for systems;
- Ensures that the authorizing official authorizes systems for processing before commencing operations; and
- Updates the security authorization.

TTUHSC El Paso requires all new technology platforms to be approved by the IT Security team prior to the introduction of new systems in production environments. Unauthorized systems:

a. Are prohibited from operating in a production environment;
b. May be disconnected from the network and/or powered off; and
c. Must meet CIS Level 1 baseline/configuration hardening standards.

## CA-07: Continuous Monitoring

TTUHSC El Paso establishes a continuous monitoring strategy and implements a continuous monitoring

program that inclues:

- A configuration management process for systems;
- A determination of the security impact of changes to systems and the environment of operation;
- Ongoing security control assessments in accordance with organizational continuous monitoring strategy; and
- Reporting the security state of systems to appropriate organizational officials.

TTUHSC El Paso's IT management is required to assign a senior individual with technical experience the responsibility to monitor the effectiveness of TTUHSC El Paso's information security controls.

Continuous Monitoring Includes:

**Independent Assessment**
TTUHSC El Paso employs assessors or assessment teams with reasonable independence to monitor the security controls in the information system on an ongoing basis.

## CA-09: Internal System Connections

TTUHSC El Paso:

- Authorizes internal connections of systems; and
- Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

For critical systems, all internal connections must be documented and authorized.

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

1. MA201CMR17 17.03(2)(h) | OR646A.622(b)(B)(i)-(iv) | NIST CSF ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3
2. NIST CSF I.AM-3 & DE.AE-1
3. PCI DSS 1.3, 1.3.3 & 1.3.5
4. PCI DSS 1.3, 1.3.3 & 1.3.5
5. PCI DSS 1.3.1, 1.3.2 & 1.3.4
6. PCI DSS 1.2.3
7. OR646A.622(b)(B)(iii) | NIST CSF ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.AN-1, RS.CO-3 & RS.MI-3
8. PCI DSS 11.3-11.3.3 | NIST CSF ID.RA-1
9. TAC §202.74, TAC §202.75

*Revised May 2018*