HSCEP OP: 56.50 - Risk Assessment (RA)

Policy Statement:

TTUHSC El Paso shall periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

Reason for Policy:

The purpose of the Risk Assessment (RA) 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 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: risk assessment policy & procedures, security categorization, risk assessment and update, vulnerability scanning, and technical surveillance countermeasures security.

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 56.01.10 Disciplinary Process.

RA-01: Risk Assessment Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

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

TTUHSC El Paso is required to identify and document organization-wide security risk assessment controls that, at a minimum, include:

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

RA-02: Security Categorization

TTUHSC El Paso:

- Categorizes systems and data in accordance with applicable local, state, and Federal laws;
- Documents the security categorization results (including supporting rationale) in the security plan for systems; and
- Ensures the security categorization decision is reviewed and approved by the asset owner.

Based on the System Criticality and Data Sensitivity of a system, asset custodians and data/process owners are required to:

a. Categorize the system and data; and
b. Where applicable, document the security categorization results (including supporting rationale) in a System Security Plan (SSP) for the system.

RA-03: Risk Assessment

TTUHSC El Paso:

- Conducts an annual assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits;
- Documents risk assessment results in an organization-approved format; and
- Reviews risk assessment results.

a. At least once per year or upon significant changes to the networks, TTUHSC El Paso is required to conduct a formal information security risk assessment for the corporate network that, at the very least, covers the following:

    i. Identifies
    ii. Critical assets;
    iii. Potential natural and man-made threats;
    iv. Vulnerabilities;
b. Documents known vulnerabilities in a formal risk assessment; and
c. Assesses current information security controls affecting the confidentiality, integrity, and availability of critical data.

Risk Assessment includes:

Risk Ranking
TTUHSC El Paso will establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry-recognized leading practices.

Asset custodians and data/process owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system.

RA-05: Vulnerability Scanning

TTUHSC El Paso:

- Scans for vulnerabilities in systems and hosted applications annually, and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
    - Enumerating platforms, software flaws, and improper configurations;
    - Formatting and making transparent, checklists and test procedures; and
    - Measuring vulnerability impact;
- Analyzes vulnerability scan reports and results from security control assessments;
- Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and
- Shares information obtained from the vulnerability scanning process and security control assessments

with designated personnel throughout the organization to help eliminate similar vulnerabilities in other systems (e.g., systemic weaknesses or deficiencies).

TTUHSC El Paso's IT security personnel are responsible for the following vulnerability scanning-related activities:

a. Perform ongoing scans for vulnerabilities in systems and hosted applications, as well as ad hoc scans when new vulnerabilities potentially affecting system(s)/application(s) are identified and reported;
b. Utilize vulnerability scanning tools and techniques that promote:
   i. Enumerating platforms, software flaws, and improper configurations;
   ii. Formatting and making transparent, checklists and test procedures; and
   iii. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results;
d. Remediate legitimate vulnerabilities in accordance with a risk-based approach; and
e. Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout TTUHSC El Paso to help eliminate similar vulnerabilities in other systems (e.g., systemic weaknesses or deficiencies).

Vulnerability Scanning includes:

Update Tool Capability
TTUHSC El Paso must employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Update by Frequency/Prior to New Scan/When Identified
TTUHSC El Paso must update the information system vulnerabilities scanned:

a. Automatically
b. Prior to a new scan; and/or
c. When new vulnerabilities are identified, and reported.

Breadth/Depth of Coverage
TTUHSC El Paso must employ vulnerability scanning mechanisms that are capable of:

a. Covering the appropriate scope of assets that require scanning; and
b. Being able to identify known vulnerabilities on scanned assets.

Privileged Access
Where technically feasible, information systems must implement privileged access authorization for selected vulnerability scanning activities.

Automated Trend Analysis
Where technically feasible, TTUHSC El Paso shall employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Review Historical Audit Logs
Where technically feasible, TTUHSC El Paso security personnel must review historical audit logs to determine if identified vulnerabilities were exploited on TTUHSC El Paso assets.

External Vulnerability Assessment Scans for PCI DSS Compliance
For standards within scope for PCI DSS, TTUHSC El Paso is required to perform external network vulnerability scans, via an Approved Scanning Vendor (ASV), at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

Internal Vulnerability Assessment Scans for PCI DSS Compliance
For assets within scope for PCI DSS, TTUHSC El Paso is required to perform internal network

vulnerability scans at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all "High" vulnerabilities as defined in the PCI DSS are resolved.

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

56.50 Disciplinary Process (DI)
NIST CSF ID.AM-3 & PR.IP-2
MA201CMR17 17.03(2)(b)
PCI DSS 9.6.1 | NIST CSF ID.AM-5, ID.RA-4 & ID.RA-5
HIPAA 164.308(a)(1)(ii)(A) & (B) | GLBA Safeguards Rule | PCS DSS 12.2 | MA201CMR17 17.03(2)(b) | OR64A.622(b)(A)(ii) | NIST CSF ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3
National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS)
http://nvd.nist.gov/cvss.cfm
GLBA Safeguards Rule | PCI DSS 6.1 | MA201CMR17 17.03(2)(i) & 17.03(2)(b)(c) | OR646.622 (b)(A)(iv)
PCI DSS 11.2 | OR646A.622(b)(B)(iii) & OR646A.622(b)(d)(A)(iii) | NIST CSF ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3 & RS.MI-3
PCI DSS 11.2, 11.2.2 & 11.2.3
PCI DSS 11.2, 11.2.1 & 11.2.3
TAC §202.74, §202.75

Revised May 2018