HSCEP OP: System & Information Integrity (SI)

Policy Statement:

TTUHSC El Paso shall correct flaws in its systems in a timely manner and ensure mechanisms are in place to protect systems from malicious code.

Reason for Policy:

The purpose of the System & Information Integrity (SI) policy is to ensure the confidentiality, integrity, and availability of TTUHSC El Paso's data.

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 System & Information Integrity, Flaw Remediation, malicious code, information system monitoring, security alerts, advisories & directives, functionality verification, software & firmware integrity, spam protection, input restrictions, input data validation, error handling, output handling & retention, predictable failure analysis, non-persistence Information Output filtering, memory protection, and fail-safe procedures.

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.

SI-01: System & Information Integrity Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented system and information integrity 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 system and information integrity policy and associated system and information integrity controls.

TTUHSC El Paso is required to document TTUHSC El Paso-wide system and information integrity controls that, at a minimum include:

a. A formal, documented system and information integrity policy; and
b. Processes to facilitate the implementation of the system and information integrity policy, procedures and associated controls.

SI-02: Flaw Remediation (Software Patching)

TTUHSC El Paso:

- Identifies, reports, and corrects system flaws;
- Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational systems before installation; and
- Incorporates flaw remediation into the organization's configuration management process.

Asset custodians and data/process owners are required to ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed:

a. Install applicable, critical security patches within one (1) month of release from the vendor; and
b. Install applicable, non-critical patches within three (3) months of release from the vendor.

Flaw Remediation includes:

Centralized Management
Asset custodians and data/process owners are required to centrally manage the flaw remediation process that includes, but is not limited to the following:

a. Documentation of impact;
b. Documented change approval by authorized parties;
c. Functionality testing to verify that the change does not adversely impact the security of the system;

Automated Flaw Remediation Status
Where technically feasible, TTUHSC El Paso shall employ automated mechanisms to determine the state of information system components with regard to flaw remediation.

Time to Remediate Flaws/Benchmarks for Corrective Action
Where technically feasible, TTUHSC El Paso shall collect metrics associated with flaw remediation and provide metrics reports to key stakeholder

SI-03: Malicious Code Protection (Malware)

TTUHSC El Paso:

- Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
  - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
  - Inserted through the exploitation of system vulnerabilities;
- Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;
- Configures malicious code protection mechanisms to:
  - Perform periodic scans of the system and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
  - Quarantines malicious code; send alert to an administrator; in response to malicious code detection; and
- Addresses the receipt of false positives during malicious code detection.

TTUHSC El Paso is required to deploy anti-malware software on all systems commonly affected by malicious software, including but not limited to:

a. Servers;
b. Workstations;
c. Laptops;
d. Tablets; and
e. Smartphones.

Malicious Code Protection includes:

Centralized Management
TTUHSC El Paso's IT security personnel are responsible for selecting and implementing the approved application for centrally managing host-based, malicious code protection mechanisms.

Automatic Updates
Asset custodians are required to ensure anti-malware software is configured to automatically update malicious code protection mechanisms.

Nonsignature-Based Detection
Where technically feasible, TTUHSC El Paso shall implement nonsignature-based malicious code detection mechanisms.

Malware protection mechanism Testing
Asset custodians are required to use the European Institute of Computer Anti-Virus Research (EICAR) Standard Anti-Virus Test File to ensure anti-malware software is properly detecting and removing threats.

Evolving Malware Threats
TTUHSC El Paso's IT security personnel are responsible for developing and implementing the process for periodic evaluations to identify and evaluate evolving malware threats for systems considered to be not commonly affected by malicious software.

Always On Protection
TTUHSC El Paso's IT security personnel are responsible for ensuring that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period.

SI-04: Information System Monitoring

TTUHSC El Paso:

- Monitors events on systems in accordance with organization-defined monitoring objectives and detects system attacks;
- Identifies unauthorized use of systems; and
- Heightens the level of system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, or other organizations, based credible sources of information.

TTUHSC El Paso management is responsible for developing and implementing daily, operational information security procedures that are consistent with legal and contractual requirements.

Information System Monitoring includes:

System-Wide Intrusion Detection Systems
Where technically feasible, TTUHSC El Paso shall connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.

Automated Tools for Real-Time Analysis
For critical systems, TTUHSC El Paso IT security personnel are responsible for correlating information and generating near real-time alerts from monitoring tools employed throughout the network to achieve organization-wide situational awareness.

Inbound & Outbound Communications Traffic
TTUHSC El Paso is required to monitor inbound and outbound communications for unusual or unauthorized activities or conditions.

System Generated Alerts
TTUHSC El Paso is responsible for developing and implementing an integrated situational awareness capability

to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out the attacks.

Wireless Intrusion Detection
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

Correlate Monitoring Information
TTUHSC El Paso shall correlate information from monitoring tools employed throughout the organization.

Host-Based Devices
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall implement host-based monitoring mechanisms on information system components.

SI-05: Security Alerts, Advisories & Directives

TTUHSC El Paso:

- Receives system security alerts, advisories, and directives from designated external organizations on an ongoing basis; and
- Generates internal security alerts, advisories, and directives as deemed necessary.

TTUHSC El Paso IT security personnel responsible for incident response operations are required to utilize automated mechanisms to receive security alert and advisory information.

SI-07: Software, Firmware & Information Integrity

Systems detect unauthorized changes to software and information.

On critical systems, asset custodians are required to:

a. Deploy File Integrity monitoring (FIM) tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly;
b. Verify the use of FIM tools by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:

    1. System executables;
    2. Application executables;
    3. Configuration and parameter files; and
    4. Centrally stored, historical or archived, log and audit files.

c. Verify the tools are configured to alert personnel to unauthorized modification of critical files and to perform critical file comparisons at least weekly.

Software, Firmware & Information Integrity includes:

Integrity Checks
Where technically feasible, TTUHSC El Paso system will perform an integrity check of organization-defined software, firmware, and information at:

a. Startup; or
b. Upon security-related events.

Integration of Detection & Response
Where technically feasible, TTUHSC El Paso shall incorporate the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability.

SI-08: Spam Protection

TTUHSC El Paso:

- Employs spam protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
- Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

TTUHSC El Paso is required to centrally manage spam protection mechanisms, including signature definitions, in an effort to reduce the introduction of malicious software to clients' systems.

Spam Protection includes:

Central Management
Where technically feasible, TTUHSC El Paso shall centrally manage the spam protection mechanisms.

Automatic Updates
Where technically feasible, information systems must automatically update spam protection mechanisms.

SI-10: Input Data Validation

TTUHSC El Paso systems check the validity of information inputs.

On custom-developed applications and web pages, asset custodians and data/process owners are required to enforce rules for checking the valid syntax and semantics of system inputs are in place to verify that inputs match specified definitions for format and content. System inputs include, but are not limited to:

a. Character set;
b. Length;
c. Numerical range; and
d. Acceptable values.

SI-11: Error Handling

TTUHSC El Paso:

- Identify potentially security-relevant error conditions;
- Generate error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and
- Reveal error messages only to authorized personnel.

Asset custodians and data/process owners are required to examine the structure and content of error messages to identify how error conditions are handled for systems.

SI-12: Information Output Handling & Retention

TTUHSC El Paso:

- handles and retains both information within and output from systems in accordance with applicable local, state, and Federal laws, as well as regulatory requirements.

TTUHSC El Paso is required to design, implement and maintain a data retention program for the systematic retention and destruction of physical and digital documents based on statutory and regulatory record-keeping requirements and practical business needs that include:

a. Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements;
b. Processes for secure deletion of data when no longer needed;

c. Specific retention requirements for cardholder data; and
d. A quarterly process (automatic or manual) for identifying and securely deleting stored sensitive data that exceeds defined retention requirements.

SI-16: Memory Protection

TTUHSC El Paso systems implement security safeguards to protect system memory from unauthorized code execution.

Asset custodians and data/process owners are required to configure critical systems to protect system memory from unauthorized code execution.

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

56.50 Disciplinary Process (DI)
PCI DSS 6.1 & 6.2 | MA201CMR17 17.04(6) | OR646A.622(2)(B)(iii) | NIST CSF ID.RA-1 & PR.IP-12
PCI DSS 6.2, 6.4.5, 6.4.5.1-6.4..5.4 & 6.4.6 | MA201CMR17 17.04(7)
HIPAA 164.308(a)(5)(ii)(B) | PCI DSS 5.1, 5.1.1 & 5.2 | MA201CMR17 17.04(7) | NIST CSF DE.CM-4 & DE.DP-3
PCI DSS 5.2
PCI DSS 5.1.2
PCI DSS 5.3
HIPAA 164.308(a)(1)(ii)(D) & 164.308(a)(5)(ii)(C) | PCI DSS 11.4 | MA201CMR17 17.03(2)(b)(c) & 17.04(4) | NIST CSF ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-5, DE.CM-6, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 & RS.CO-3
PCI DSS 10.6, 10.6.1, 10.6.2 & 10.6.3
PCI DSS 11.1
OR646A.622.(2)(d)(B)(iii) | NIST CSF ID.RA-1, ID.RA-2, ID.RA-3 & RS.CO-5
PCI DSS 11.5 & 11.5.1 | NIST CSF PR.DS-6
PCI DSS 3.1 & 10.7 | OR646A.622(b)(C)(i) & (iv)
OR646A.622(2)(d)(C)(iii)
TAC §202.74, §202.75

Revised May 2018