HSCEP OP: 56.50 - Sanctions Policy (SN)

Policy Statement:

TTUHSC El Paso shall employ industry-recognized leading practice principles that promote effective IT security within systems and the network.

Reason for Policy:

The purpose of the System & Communication Protection (SC) policy is to ensure sufficient protections are in place to protect the confidentiality and integrity of TTUHSC El Paso's communications to align with CIS level 1 baseline/configurations for hardening.

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: policy & procedures, application partitioning, information in shared resources, denial of service (DoS) protection, Transmission Confidentiality, Use of Cryptography, session authenticity, communications technologies, encrypting data at rest, distributed processing & storage, wireless link protection, usage restrictions, and multiple other areas of system & communication protection.

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 sanctions as outlined in this policy, and according to the policy rating scale below. In addition to departmental disciplinary action, violations may be subject to penalty under federal, state, and local legislation.

Policy Violation as applied

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

Per Compliance policy HSCEP OP 52.04 on internal investigation of alleged violations, each incident that is reported will follow thorough investigative procedure.

SC-01: System & communications Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented system and communications protection 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 communications

protection policy and associated system and communications protection controls.

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

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

SC-02: Application Partitioning

System configurations separate user functionality (including user interface services) from system management functionality.

Where technically feasible, physically or logically separate user interfaces (e.g., administrative or database management). Separation may be accomplished through the use of one or more of the following:

a. Network segmentation;
b. Different computers;
c. Different central processing units;
d. Different instances of the operating system;
e. Different network addresses; or
f. Other methods as appropriate.

SC-04: Information In Shared Resources

Systems prevent unauthorized and unintended information transfer via shared system resources.

Asset custodians and data/process owners are required to ensure that systems are configured to require privilege levels for access. The levels must ensure data is not exposed to individuals or processes with a lower privilege level.

SC-05: Denial of service (DoS) Protection

TTHUSC El Paso systems protect against or limit the effects of denial of service attacks.6

Technology architects, asset custodians, and data/process owners are required to configure the architecture of the network and systems to ensure the capability exists to limit the effects of denial of service attacks.

SC-07: Resource Priority

TTUHSC El Paso employs boundary protection mechanisms to separate system components directly supporting organization-defined missions and/or business functions.

Network administrators are required to:

a. Implement a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the internal network zone;
b. Verify that the current network diagrams are consistent with the firewall configuration standards;
c. Prohibit direct public access between the Internet and any sensitive system in the internal network zone;
d. Restrict inbound and outbound traffic to that which is necessary for authorized business purposes;
e. Limit the number of access points to the system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;
f. Ensure traffic flow policies are established and reviewed for each managed interface;
g. Ensure the exceptions to Access Control Lists (ACLs) are documented and reviewed;
h. Ensure systems prevent remote devices that have established a non-remote connection (e.g., VON) with the system from communicating outside that path and with resources external to the network;
i. Ensure systems prevent the unauthorized release of information outside the system boundary or any unauthorized communication through the system boundary when there is an operational failure of the

boundary protection mechanisms;

j. Ensure private IP addresses and routing information are not disclosed to unauthorized parties; and
k. Implement a firewall between any wireless networks and the internal network zone:
   i. Verify that there are perimeter firewalls installed between any wireless networks and systems that store sensitive data;
   ii. Configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the internal network zone; and
   iii. Verify that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Boundary Protection includes:

Access Points
Where technically feasible, asset custodians and asset owners must limit the number of external network connections to the information system.

External Telecommunications Services
TTUHSC El Paso must:

a. Implement a managed interface for each external telecommunication service;
b. Establish a traffic flow policy for each managed interface;
c. Protect the confidentiality and integrity of the information being transmitted across each interface;
d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
e. Review exceptions to the traffic flow policy and removes exceptions that are no longer supported by an explicit mission/business need.

Deny Traffic by Default & Allow Traffic by Exception
An explicit "deny all" or an implicit deny after allow statement is required to ensure that all unnecessary inbound and outbound traffic is denied by default.

Prevent Split Tunneling for Remote Devices
Asset custodians are required to configure information systems to prevent "split tunneling" for remote devices.

Route Traffic To Proxy Servers
TTUHSC El Paso prohibits direct public access between the Internet and any system on TTUHSC El Paso's internal networks.

Host-Based Protection
TTUHSC El Paso requires:

a. The installation of firewall software or equivalent functionality on any Internet-accessible mobile device or computer;
b. Verification that the firewall software is configured to specific standards and is not alterable by users of the mobile and/or employee-owned computers; and
c. The installation of a Web Application Firewall (WAF) in front of sensitive, public-facing web applications detect and prevent web-based attacks.

Isolation of Security Tools/Mechanisms/Support Components
Where technically feasible, TTUHSC El Paso shall isolate information security tools, mechanisms, and support components from other internal information system components by implementing physically separate subnetworks.

Internal Network Address Space
Asset custodians and data/process owners are required to configure systems to prevent the disclosure of

private IP addresses and routing information to unauthorized parties. methods to obscure IP addressing may include, but are not limited to:

a. Network address Translation (NAT);
b. Placing systems behind proxy servers/firewalls or content caches;
c. Removing or filtering route advertisements for private networks that employ registered addressing; or
d. Using internal use of RFC1918 address space instead of registered addresses.

Fail Secure
Where technically feasible, asset custodians and data/process owners are required to configure assets to fail in a known state for types of failures in order to preserve system state information at the time of the failure.

SC-08: Transmission Confidentiality and Integrity

TTUHSC El Paso protects the integrity of transmitted information.

Asset custodians and data/process owners are required to prevent unauthorized disclosure of information during transmission, ensuring systems transmitting sensitive information:

a. Only trusted keys and certificates are accepted;
b. Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;
   i. Examples of public networks include, but are not limited to:
      1. The Internet;
      2. Wireless technologies;
      3. Global System for Mobile communications (GSM); and
      4. General Packet Radio Service (GPRS).
   ii. Examples of private networks include, but are not limited to:
      1. Local Area Networks (LAN); and
      2. Virtual Private Network (VPN).
c. Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices; and
d. Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations. For TLS implementations:
   i. Verify that HTTPS appears as a part of the browser Universal Record Locator (URL); and
   ii. Verify that no sensitive data is required when HTTPS does not appear in the URL.

Transmission Confidentiality and Integrity includes:

Cryptographic or Alternate Physical Protection
Unless otherwise protected by TTUHSC El Paso-defined alternative physical safeguards, information systems must:

a. Implement cryptographic mechanisms to prevent unauthorized disclosure of information; and
b. Detect changes to information during transmission.

SC-09: Transmission Confidentiality

Absorbed into SC-08

SC-10: Network Disconnect

Systems terminate remote sessions at the end of the session or after an organization-defined time period of inactivity.

Asset custodians and data/process owners are required to configure systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than fifteen (15)

minutes.

SC-12: Cryptographic Key Establishment & Management

TTUHSC El Paso establishes and manages cryptographic keys for required cryptography employed within systems.

Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

a. Protect any keys used to secure sensitive data against disclosure and misuse;
b. Restrict access to cryptographic keys to the fewest number of custodians necessary;
c. Store cryptographic keys securely in the fewest possible locations and forms; and
d. Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption, including the following:
   i. Generation of strong cryptographic keys;
   ii. Secure cryptographic key distribution; and
   iii. Secure cryptographic key storage; and
e. Maintain a documented description of the cryptographic architecture that includes:
   i. Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date;
   ii. Description of the key usage for each key; and
   iii. Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management.

Cryptographic Key Establishment & Management includes:

Symmetric Keys
Where technically feasible, TTUHSC El Paso shall produce, control, and distribute symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes.

Asymmetric Keys
Where technically feasible, TTUHSC El Paso shall produce, control, and distribute asymmetric cryptographic keys using approved key management technology and processes that protect the user's private key.

Cryptographic Key Loss or Change
Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

1. Change cryptographic keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry-recognized leading practices and guidelines;
2. Retire or replace (e.g., archive, destroy and/or revoke) keys as deemed necessary when the integrity of the key has been weakened (e.g., departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised; and
3. Use archived cryptographic keys only for decryption/verification purposes.

Control & Distribution of Cryptographic Keys
Asset custodians responsible for Public Key Infrastructure (PKI) are required to:

a. Use split knowledge and dual control (e.g., require two or three people, each knowing only their own key component, to reconstruct the whole key) if manual, clear-text cryptographic key management operations are used. Examples of manual key management operations include, but are not limited to:
   1. Key generation;
   2. Transmission;
   3. Loading;

4. Storage; and
5. Destruction.

b. Prevent the unauthorized substitution of cryptographic keys; and
c. Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

SC-13: Use of Cryptography

Systems implement required cryptographic protections using cryptographic modules that comply with applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound to address.

Asset custodians and data/process owners are required to ensure systems storing, processing or transmitting sensitive information:

a. Employ cryptographic mechanisms;
b. Use strong cryptography and security protocols (for example, TLS, IOSEC, SSH, etc.) to safeguard sensitive data during transmission over public or private networks;
c. Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices; and
d. Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.

SC-15: Collaborative Computing Devices

TTUHSC El Paso systems prohibit remote activation of collaborative computing devices with the following exceptions:

- Networked whiteboards;
- Cameras; and
- Microphones.

Asset custodians and data/process owners are required to configure systems to provide an explicit indication of use that includes signaling to users when collaborative computing devices are activated.

SC-17: Public Key Infrastructure (PKI) Certificates

TTUHSC El Paso issues public key certificates under an organization-defined certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Asset custodians responsible for publicly-facing Public Key Infrastructure (PKI) are required to provide the following PKI management services:

a. Certificate creation;
b. Certificate signing;
c. Certificate revocation;
d. Key management;
e. Publication of certificate revocation lists (CRLs); and
f. Authority revocation lists (ARLs).

SC-18: Mobile Code

TTUHSC El Paso:

- Defines acceptable and unacceptable mobile code and mobile code technologies;
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorizes, monitors, and controls the use of mobile code within systems.

Asset custodians and data/process owners are required to manage the use of mobile code technologies through:

- Defining acceptable and unacceptable mobile code and mobile code technologies;
- Establishing usage restrictions for mobile code and mobile code technologies; and
- Developing secure systems configurations to address mobile code usage within systems that include, but is not limited to:
  i. Preventing the download and execution of prohibited mobile code; and
  ii. Preventing the automatic execution of mobile code.

SC-19: Communication Technologies

TTUHSC El Paso establishes usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.

Human Resources (HR) is responsible for establishing usage restrictions and implementation guidance for the following communications technologies based on the potential to cause damage to systems, if used maliciously:

a. Electronic Mail (email);
b. Instant Messaging (IM);
c. Short Message Service (SMS);
d. Voice Over Internet Protocol (VOIP);
e. Analog Lines (Plain Old Telephone Service (POTS); and
f. Facsimile (FAX) Machines (analog & digital).

SC-20: Secure Name/Address Resolution Service (Authoritative Source)

TTUHSC El Paso systems provide additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

TTUHSC El Paso is required to use trusted sources for authoritative DNS queries to prevent DNS spoofing attacks.

SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

TTUHSC El Paso systems perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Asset custodians are required to configure internal DNS queries to use recursive or cached name resolution.

SC-22: Architecture & Provisioning for Name/Address Resolution Service

TTUHSC El Paso systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Asset custodians responsible for Domain Name System (DNS) are required to:

a. Ensure DNS Servers providing name/address resolution service are fault tolerant and implement internal/external role separation;
b. Ensure primary and secondary authoritative DNS servers are on separate subnets at separate locations;
c. Ensure DNS servers with an internal role only process name/address resolution requests from internal clients; and
d. Ensure DNS servers with an external role only process name/address resolution requests from external clients.

SC-23: Fail in Known State

TTUHSC El Paso systems provide mechanisms to protect the authenticity of communications sessions.

Where technically feasible and a business reason exists, TTUHSC El Paso is required to implement authenticity protection mechanisms to protect the integrity of session communications.

SC-28 Encrypting Data At Rest

TTUHSC El Paso systems protect the confidentiality and integrity of information at rest.

Asset custodians and data/process owners are required to protect sensitive information by:

a. Employing cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
b. Rendering sensitive data unreadable anywhere it is stored; and
c. Not trying user accounts to decryption keys.

Encrypting Data at Rest includes:

Cryptographic Protection
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of information on information system components.

SC-39 Process Isolation

TTUHSC El Paso system maintains a separate execution domain for each executing process.

Where technically feasible and a strong business need exists, asset custodians are required to implement a separate execution domain for each executing process.

Process Isolation includes:

Hardware Separation
Where technically feasible and a strong business need exists, asset custodians are required to configure systems to implement underlying hardware separation mechanisms to facilitate process separation.

Thread Separation
Where technically feasible and a strong business need exists, asset custodians are required to configure systems to maintain a separate execution domain for each thread in multi-threaded processing.

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

56.50, Sanctions Policy (SN)
PCI DSS 11.3.4
PCI DSS 1.2, 1.3.1, 2.2.1, & 11.3.4
PCI DSS 11.3.4 & 11.3.4.1
PCI DSS 1.3.7
NIST CSF PR.DS-4 & DE.CM-1
PCI DSS 1.1.3, 1.1.4, 1.2.1, 1.2.3 & 1.3 | MA201CMR17 17.04(6) | NIST CSF PR.AC-5, PR.DS-5, PR.PT-4 & DE.CM-1
PCI DSS 1.2.1
PCI DSS 1.3
PCI DSS 1.4
PCI DSS 1.3.8
NIST 800-53 SC-7(18)
HIPAA 164.312(e)(2)(i) | PCI DSS 4.1 | PR.DS-2 & PR.DS-5

HIPAA 164.312(e)(1) & 164.312(e)(2)(i) | MA201CMR17 17.04(3) | OR646A.622(2)(d)(C)(iii)
PCI DSS 8.1.8
PCI DSS 3.5, 3.5.1-3.5.4, 3.6 & 3.6.1-3.6.3
PCI DSS 3.6.4 & 3.6.5
PCI DSS 3.6.6-3.6.8
HIPAA 164.312(e)(2)(ii) | PCI DSS 2.2.3 & 4.1 | NIST CSF PR.DS-5
NIST CSF DE.CM-5
Google DNS - http://code.google.com/speed/public-dns/docs/using.html
HIPAA 164.312(a)(b)(iv) | PCI DSS 3.4 & 3.4.1 | MA201CMR17 17.04(5) | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.DS-1
NIST CSF PR.DS-5
PCI-DSS 11.1 & 11.1-11.1.2
NIST CSF DE.CM-5
TAC §202.74, TAC §202.74

Revised May 2018