HSCEP OP: 56.50 - Physical & Environmental Protection (PE)

Policy Statement:

TTUHSC El Paso shall implement physical access controls to limit access to systems, equipment, and the respective operating environments to authorized individuals. TTUHSC El Paso shall provide appropriate environmental controls in facilities containing systems.

Reason for Policy:

The purpose of the Physical & Environmental Protection (PE) policy is to minimize risk to TUHSC El Paso systems and data by addressing applicable physical security and environmental concerns.

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: Access authorizations, role-based physical access, identification, unescorted access, laptop & workstation security, transmission medium, output devices, surveillance, visitor control, records, power equipment, emergency power & shutoff, fire protection, humidity controls, water damage, delivery & removal, alternate worksite, location of system components, Information Leakage, and asset tracking.

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.

PE-01: Physical & Environmental Protection Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- a formal, documented physical and environmental 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 physical and environmental protection policy and associated physical and environmental protection controls.

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

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

PE-02: Physical Access Authorizations

TTUHSC El Paso:

- Develops and keeps a current list of personnel with authorized access to the facility where the system resides (except for those areas within the facility officially designated as publicly accessible);
- Issues authorization credentials; and
- Reviews and approves the access list and removes from the access list personnel no longer requiring access.

TTUHSC El Paso is required to:

a. Develop and keeps current a list of personnel with authorized access to its facilities, except for those areas within the facility officially designated as publicly accessible;
b. Issue authorization credentials for physical access; and
c. Review and approve the access list and remove personnel no longer requiring access.

Physical Access Authorization includes:

Role-Based Access
TTUHSC El Paso is required to authorize physical access to its facilities based on position or role.

Identification Requirement
TTUHSC El Paso requires at least one (1) form of government-issued photo identification to gain access.

Restrict Unescorted Access
TTUHSC El Paso is required to restrict physical access to the systems equipment and records storage.

PE-03: Physical Access Control

TTUHSC El Paso:

- Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the system resides (excluding those areas within the facility officially designated as publicly accessible);
- Verifies individual access authorizations before granting access to the facility;
- Controls entry to the facility containing the system using physical access devices and/or guards;
- Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
- Secures keys, combinations, and other physical access devices; and
- Changes combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

TTUHSC El Paso is required to:

a. Use video cameras and/or access control mechanisms to limit and monitor physical access to the facility and systems;
b. Enforce physical access authorizations for all physical access points (including designated entry/exit points) to company-owned or operated facilities;
c. Verify individual access authorizations before granting access to the facility;
d. Control access to areas based on the physical security zone requirements;
e. Secure keys, combinations, and other physical access devices;
f. Change combinations and keys and when keys are lost, when combinations are compromised, or when individuals are transferred or terminated; and
g. Issues visitors a physical token (e.g., a badge or access device) that:
    i. Identifies the visitors as not onsite personnel;
    ii. Must be surrendered before leaving the facility or at the date of expiration; and

iii. Expires through automated or visual means (e.g., different color for each day).

Physical Access Control includes:

Lockable Physical Casings
TTUHSC El Paso is required to protect sensitive systems from physical tampering or alteration of hardware components by utilizing lockable physical casings.

Laptop Storage in Automobiles
When traveling with TTUHSC El Paso-issued laptops and mobile devices, users are required to:

a. Lock the device(s) in the trunk of a user's automobile; or
b. Maintain physical control and not leave the device(s) in the automobile.

Workstation Security
TTUHSC El Paso requires the following workplace security precautions:

a. Physical media must be properly disposed of, in accordance with document destruction policies;
b. All work areas must be cleared of all media containing sensitive data when not occupied;
c. Filing cabinets, lockable drawers / overhead cabinets, storage rooms, and any other storage unit containing sensitive data will be locked when not in use; and
d. Whiteboards, dry-erase boards, cork boards, writing tablets, and similar common shared work areas will be sanitized (e.g., erased, removed, or shredded) when not in use.

Physical Access Logs
TTUHSC El Paso is required to configure access control systems to log the following information:

a. Physical location of the access;
b. Direction of access, if possible (e.g., ingress or egress);
c. Identity of the person accessing the location; and
d. Indication of success or failure.

PE-04: Access Control for Transmission Medium

TTUHSC El Paso controls physical access to system distribution and transmission lines within organizational facilities.

TTUHSC El Paso management is required to limit physical access to transmission medium to only authorized personnel.

PE-05: Access Control for Output Devices

Physical access to system output devices must be limited to authorized personnel to prevent unauthorized individuals from obtaining the output.

Physical access to system output devices must be limited to authorized personnel to prevent unauthorized individuals from obtaining access to unsecured data.

PE-06: Monitoring Physical Access

TTUHSC El Paso:

- Monitors physical access to the system to detect and respond to physical security incidents;
- Reviews physical access logs; and
- Coordinates results of reviews and investigations with the organization's incident response capability.

TTUHSC El Paso is responsible for:

- Investigating and responding to detected physical security incidents, according to documented procedures;
- Performing security checks at the physical boundary of the facility or system for unauthorized exfiltration of information or system components;
- Using video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas;
- Reviewing collected data and correlate with other entries; and
- Retaining physical access data for at least three (3) months, unless otherwise restricted by law.

Monitoring physical access includes:

Intrusion Alarms/Surveillance Equipment
Where technically feasible, potential physical ingress and egress points will be monitored with physical intrusion alarms and surveillance equipment.

PE-07: Visitor Control

Addressed in PE-2 and PE-3.

PE-08: Access Records

TTUHSC El Paso

- Maintains visitor access records to the facility where the system resides (except for those areas within the facility officially designated as publicly accessible); and
- Reviews visitor access records.

TTUHSC El Paso is required to:

a. Use a visitor log to maintain a physical audit trail of visitor activity;
b. At a minimum, document the visitor's name, the company represented, and the onsite personnel authorizing physical access; and
c. Retain this log for a minimum of three months, unless otherwise restricted by law.

PE-09: Power Equipment & Power Cabling

TTUHSC El Paso protects power equipment and power cabling for the system for damage and destruction.

Asset custodians are required to protect power equipment and power cabling from damage, tampering, and destruction.

Power Equipment & Cabling includes:

Automatic Voltage Controls
Asset custodians are required to employ automatic voltage controls for critical system components.

PE-10: Emergency Shutoff

TTUHSC El Paso:

- Provides the capability of shutting off power to the system or individual system components in emergency situations;
- Places emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and
- Protects emergency power shutoff capability from unauthorized activation.

In data center environments, asset custodians are required to:

a. Provide the capability of shutting off power to systems in emergency situations;

b. Place emergency shutoff switches or devices in close proximity to systems or systems components to facilitate safe and easy access for personnel; and
c. Protect emergency power shutoff capability from unauthorized activation.

PE-11: Emergency Power

TTUHSC El Paso provides a long-term alternate power supply for the system that is self-contained and not reliant on external power generation.

In data center environments, asset custodians are required to provide for a long-term alternate power supply for critical systems that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

PE-12: Emergency Lighting

TTUHSC El Paso employs and maintains automatic emergency lighting for the system that activates in the event of a power outage or disruption, and that covers emergency exits and evacuation routes within the facility.

In data center environments, asset custodians are required to provide emergency lighting for all areas within the facility supporting essential missions and business functions.

PE-13: Fire Protection

TTUHSC El Paso employs and maintains fire suppression and detection devices/systems for the system that are supported by an independent energy source.

In data center environments, asset custodians are required to ensure that its facilities undergo annual fire marshal inspections and promptly resolve identified deficiencies.

Fire Protection includes:

Fire Detection Devices
In data center environments, asset custodians are required to employ fire detection devices that activate automatically and notify organizational personnel and emergency responders in the event of a fire.

Fire Suppression Devices
Where technically feasible, TTUHSC El Paso shall employ fire suppression devices/systems that provide automatic notification of any activation.

Automatic Fire Suppression
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall employ an automatic fire suppression capability.

PE-14: Temperature & Humidity Controls

TTUHSC El Paso:

- Maintains temperature and humidity levels within the facility where the system resides; and
- Monitors temperature and humidity levels.

In data center environments, asset custodians are required to employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Temperature and Humidity Controls includes:

Monitoring with Alarms/Notifications
Where technically feasible, TTUHSC El Paso shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

PE-15: Water Damage Protection

TTUHSC El Paso protects the system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

In data center environments, asset custodians are required to employ mechanisms that, without the need for manual intervention, protect systems from water damage in the event of a water leak.

PE-16: Delivery & Removal

TTUHSC El Paso authorizes, monitors, and controls types of system components entering and exiting the facility and maintains records of those items.

Systems are prohibited from being removed from TTUHSC El Paso facilities without prior, management authorization.

PE-17: Alternate Work Site

TTUHSC El Paso:

- Employs organization-defined management, operational, and technical system security controls at alternate worksites;
- Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

TTUHSC El Paso IT Management is required to develop plans regarding alternate work sites that include:

a. System security controls at alternate work sites;
b. The effectiveness of security controls at alternate work sites; and
c. The approved means for employees to communicate with administrative personnel in case of security incidents or problems.

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

56.50, Sanctions Policy (SN)
HIPAA 164.310(a)(a)
HIPAA 164.310(a)(b)(ii) | PCI DSS 9.2 | NIST CSF PR.AC-2
HIPAA 164.310(a)(b)(iii)
PCI DSS 9.4 & 9.4.1
PCI DSS 9.3
HIPAA 164.310(a)(b)(iv) | PCI DSS 9.1, 9.1.1, 9.1.2, 9.2, 9.4.2, & 9.4.3 | MA201CMR17 17.03(2)(g) | OR646A.622(2)(d)(C)(ii) | NIST CSF PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3
PCI DSS 9.1.2 & 0.1.3 | OR646A.622(2)(C)(ii) | NIST CSF PR.AC-2
OR646.622(2)(d)(C)(ii) | NIST CSF PR.AC-2
HIPAA 164.310(c) | OR646A.622(2)(d)(C)(ii) | PCI DSS 9.1 & 9.1.1 | NIST CSF PR.AC-2, DE.CM-7, RS.AN-1 & RS.CO-3
PCI DSS 9.4.4 | OR646A.6.22(2)(d)(C)(ii)
NIST CSF ID.BE-4 & PR.AC-2
NIST CSF PR.IP-5
NIST CSF ID.BE-4
NIST CSF PR.IP-5
NIST CSF PR.IP-5
NIST CSF PR.IP-5
NIST CSF PR.IP-5
OR646A.622(2)(d)(C)(ii) | NIST CSF PR.DS-3

NIST CSF PR.IP-5
NIST CSF PR.DS-5
NIST CSF DE.CM-2 & DE.CM-7
TAC §202.71, §202.72, §202.74, §202.75

Revised May 2018