

PURPOSE

Develop policies and procedures for physical and environmental protection.

PROCESS

Physical and Environmental Protection Policy and Procedures (PE-01)

The College Information Technology Department:

- A. Develops, documents, and disseminates to information system owners:
 - 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
- B. Reviews and updates the current:
 - 1. Physical and environmental protection policy biennially; and
 - 2. Physical and environmental protection procedures annually.

Physical and Environmental Protection Policy

In coordination with the Information Systems and Police department, the information system's physical spaces shall have controls in place to restrict physical access to only authorized personnel. The physical control must be activated at minimum by a keyed lock. Preferably, the physical control activation is electronic using unique access identifiers for each authorized person. Electronic access control should track person identifiers along with date and time stamps and location for each access request.

Information system spaces include client computing preparation and repair rooms, data centers, electronic data storage spaces, network equipment processing spaces, intermediate and main distribution frames (IDF, MDF), and telecommunication demarcations.

The Information Technology department must document and track access requests and assignment. Access request must be authorized by the Division Director of Information System or Chief Information Security Officer (CISO).

Physical Access Authorizations (PE-02)

The College:

- A. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
- B. Issues authorization credentials for facility access;
- C. Reviews the access list detailing authorized facility access by individuals annually; and
- D. Removes individuals from the facility access list when access is no longer required.

The Police department administers the physical access control systems. The Information Technology department administers the badge access control systems. Approval forms are completed and approved for each individual's access.

Physical Access Control (PE-03)

The College:

- A. Enforces physical access authorizations at the physical boundary by;
 - 1. Verifying individual access authorizations before granting access to the facility; and
 - 2. Controlling ingress/egress to the facility using keyed locks or electronic access control;
- B. Maintains physical access audit logs for electronic access controlled spaces;
 - 1. Provides physical locks or electronic access control to control access to areas within the facility officially designated as publicly accessible;
 - 2. Escorts visitors and monitors visitor activity into secured information system spaces;
 - 3. Secures keys, combinations, and other physical access devices;
 - 4. Inventories electronic access annually
 - 5. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Monitoring Physical Access (PE-06)

The College:

- A. Monitors physical access to the facility where the information systems resides to detect and respond to physical security incidents;
- B. Reviews physical access logs periodically based on risk management decisions and upon occurrence potential indications of events; and
- C. Coordinates results of reviews and investigations with the organizational incident response capability.
- D. Security cameras are located at ingress and egress points where the information systems resides to record activities.

Facility Access Records (PE-08)

The College:

- A. Maintains electronic access control records to the facility where the information system resides for sixty days and
- B. Reviews electronic access control access records based on risk management decisions.

Emergency Lighting (PE-12)

The College employs and maintains automatic emergency lighting where the information system resides that activates in the event of a power outage or disruption and that covers emergency exits and evacuation route within the facility per applicable building codes.

Fire Protection (PE-13)

The College employs and maintains fire suppression and detection devices/systems where the information system resides that are supported by an independent energy source per applicable building codes.

Temperature and Humidity (PE-14)

The College:

- A. Maintains temperature and humidity levels within the facility where the information system resides at levels appropriate for equipment and personnel; and
- B. Monitors temperature and humidity levels using in-room monitoring probes with minimum and maximum alerting thresholds.

Water Damage Protection (PE-15)

The College protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Delivery and Removal (PE-16)

The College authorizes, monitors, and controls information systems containing sensitive and personally identifiable information entering and exiting the facility and maintains records of those items.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.