Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Physical and Environmental Protection**
Regulation and Procedure Number:	**URP: 04.745**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This document establishes the information security physical and environmental protection regulations and procedures. The purpose of these regulations and procedures is to mitigate Texas Woman's University's ("TWU" or "University") risks from physical security and environmental threats.

The scope of these regulations and procedures is applicable to all Information Resources owned or operated by TWU. All Users are responsible for adhering to this policy. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures. The Policy Owner, as defined in URP 01.320: University Policy Development and Implementation, is responsible for managing the development, documentation, and dissemination of this URP.

APPLICABILITY

This policy is applicable to TWU Students, Employees, University Affiliates, and Guests.

DEFINITIONS

1. "Employee" means any individual at TWU who is hired in a full-time, part-time, or temporary capacity in a faculty or staff position, or in a position where the individual is required to be a Student as a condition of employment.

2. "Critical Information Systems" include, but not limited to, servers, SANs, core routers, and core telecommunication equipment. Facilities that house Critical Information Systems are generally referred to as server rooms or data centers.

3. "Guests" mean any individual not affiliated with TWU.

4. “Information Resources” means an element of infrastructure that enables the transaction of data, designed to provide content and information services to Users. Information Resources include information in electronic, digital, or audiovisual format and any hardware or software that store and use such information (i.e., electronic mail, local databases, externally accessed, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, voice mail, faxes). This definition also includes computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, cloud services, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, Information Resources includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

5. “Information System” means a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

6. "Information System Component" means a discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an Information System.

7. “Information System Owner” means the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an Information System.

8. “Physically Secured” means locked in a location that denies access to unauthorized personnel.

9. “Student” means a person taking courses at TWU, a person who is not currently enrolled in courses but who has a continuing academic relationship with TWU, or a person who has been admitted or readmitted to TWU.

10. “University Affiliate” means any individual associated with TWU in a capacity other than as a Student or Employee who has access to TWU

resources through a contractual arrangement or other association. This includes the following individuals:

a. Contractors and Vendors: an individual, business, or governmental entity that has a fully executed contract to provide goods or services to TWU. This includes employees of contractors or vendors and independent contractors.

b. Employee of a Governmental Agency: an individual employed by a federal or Texas state agency.

c. Employee of a TWU-Affiliated Institution: an individual who works for organizations that are tightly aligned with the University.

d. Pre-Employment Individual: an individual who will be hired by the University and the hiring department has sponsored their access to TWU resources.

e. Other University Affiliate: any individual who does not fit into any other category and needs access to TWU resources.

11. "User" means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Physical Access Authorization

1. TWU shall develop, approve, and maintain a list of individuals with authorized access to facilities where Information Systems reside. Facility access is managed by the University electronic card swipe system and the centrally managed key program.

2. TWU shall issue authorization credentials (i.e. keys and TWU access cards) for facility access. It is the responsibility of the business functional area to coordinate with TWU ID Systems or Facilities Management and Construction ("FMC") to authorize appropriate facility access for the User. ID Systems and FMC shall provide TWU access cards or keys, respectively, only after proper authorization has been documented.

3. Appropriate facility access is programmed for each User's official TWU access card by TWU ID Systems. Key control is managed by FMC (*See* URP 04.530: Key Control).

4. TWU ID Systems reviews access lists on an ongoing basis. FMC shall conduct a random, annual audit of key records in accordance with URP 04.530: Key Control.

5. It is the responsibility of the business functional unit to follow applicable University Employee, Student and University Affiliate termination policies in order for facility access to be terminated (*See* URP 04.705: Information Personnel Security, and the Office of Human Resources Guide for Exiting Employees).

6. TWU ID Systems and FMC shall remove individuals from the facility access list(s) when access is no longer required.

B. Physical Access Control

1. It is the responsibility of all Users to secure their keys, combinations, and other physical access devices.

2. Business functional areas shall inventory personnel with physical access devices (e.g. keys and access cards) on a regular basis and monitor for discrepancies. Any discoveries shall be reported to the appropriate department for physical access modification or termination.

3. Non-critical Information Resources are physically secured and protected by locks that are managed by FMC.

4. ITS Critical Information Systems are physically secured and protected by card swipe access that is managed by ID Systems.

5. For facilities with ITS Critical Information Systems, the Information System Owner, or designee, shall:

   a. Enforce physical access authorization to the facility where the Critical Information System resides by:

      i. Verifying individual User access authorizations before granting access to the facility; and

      ii. Controlling ingress and egress to the facility using the card swipe system.

   b. Maintain physical access audit logs of User entry of the Critical Information System facility through the use of reporting and auditing tools;

   c. Escort and monitor Guests through facilities that contain Critical Information Systems; and

d. Request for lock change or update to the card swipe system when keys or physical access cards are lost, stolen, compromised or not turned in.

6. Guests shall have perimeter access for most University buildings during standard scheduled hours of operation. TWU ID Systems maintains records showing the standard scheduled hours of operation for University buildings and facilities and outlines access procedures in order to enhance campus safety and security. Perimeter access is managed by the card swipe system.

7. Users with authorized physical access after standard operating hours shall escort and monitor Guests through University facilities.

8. Users must report lost or stolen access cards to ID Systems and keys in accordance with URP 04.530: Key Control.

9. Exiting or terminated Users must turn in all University property, including facility access equipment prior to termination.

10. Users that transfer departments and require modified physical access shall notify their supervisor and request appropriate modification from ID Systems and FMC.

11. When access cards are reported lost, stolen, or not returned, access shall be terminated for the User by ID Systems. The User shall request a replacement access card in order to regain physical access via the card swipe system.

12. Key locks shall be re-keyed in accordance with URP 04.530: Key Control if a key is reported lost, stolen or not returned to FMC.

C. Monitoring Physical Access

1. ID Systems shall monitor physical access to the facility where ITS Critical Information Systems reside to detect and respond to physical security incidents. Entry logs are automatically captured and stored in the University's card swipe system.

2. ID Systems shall review physical access logs regularly and review system notifications upon User entry of ITS Critical Information System facilities.

3. TWU Department of Public Safety ("DPS") personnel shall conduct walk-throughs and patrols of TWU facilities to monitor, detect and respond to physical security incidents.

4. The TWU department head is responsible for coordinating results of reviews and investigations with the appropriate TWU incident response capability.

D. Visitor Access Records

The Information System Owner, or designee, shall:

1. Maintain visitor access records to the facility where ITS Critical Information Systems reside;

2. Retain records in accordance with the TWU records retention schedule;

3. Review visitor access records regularly and in response to a physical security incident; and

4. Report anomalies in visitor access records to the head of the business functional area.

E. Emergency Lighting

1. TWU shall employ and maintain automatic emergency lighting for facilities with Critical Information Systems that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

2. ITS Critical Information System facilities have battery backups and generators for emergency backup power.

3. ITS Critical Information System facilities have emergency lights that activate in the event of a power outage or disruption. These lights cover emergency exits and evacuation routes within the facility.

F. Fire Protection

1. TWU shall employ and maintain fire detection and suppression systems that are supported by an independent energy source.

2. TWU Risk Management shall ensure appropriate fire detection and suppression equipment to protect Critical Information Systems and other facilities containing Information Resources are in place in the event of a fire.

3. Fire suppression and detection systems shall:

a. Activate automatically in the event of a fire;

b. Provide automatic notification of any activation to facility inhabitants and emergency responders; and

c. Be monitored and inspected regularly by TWU Risk Management.

4. Employees shall receive training in appropriate monitoring, response and use of fire suppression equipment in case of emergencies.

G. Environmental Controls

1. TWU shall monitor temperature and humidity levels within facilities where Critical Information Systems reside and ensure that acceptable temperature and humidity levels are maintained.

2. TWU FMC shall maintain, repair, and monitor the systems that control the temperature and humidity in facilities with Critical Information Systems.

3. ITS uses an automated temperature and humidity monitoring system, and alerts are sent to the ITS. ITS then notifies the appropriate University staff to respond.

H. Water Damage Protection

1. TWU shall protect facilities with Critical Information Systems from damage resulting from water leakage by providing shutoff valves that are accessible, working properly, and known to key personnel.

2. TWU FMC ensures facilities with Critical Information Systems have master shutoff or isolation valves that are accessible and are working properly.

I. Delivery and Removal

The Information System Owner, or designee, shall:

1. Authorize and control Information System Components that are delivered to or removed from Critical Information System facilities; and

2. Document and maintain records of Information System Components delivered to or removed from Critical Information System facilities.

J. Alternate Work Site

1. Alternate work site requirements are documented in URP 05.620: Alternative Work Arrangements for Staff Employees and URP 04.700: Computer & Software Acceptable Use Policy.

2. Employees and University Affiliates at alternate work sites must adhere to TWU URPs, state, and federal regulations.

3. TWU Information Resources at alternate work sites shall be sufficiently maintained in order to validate the effectiveness of required security controls (*See* Section I.K, URP 04.700: Computer & Software Acceptable Use Policy). Employees will ensure that University owned computers are connected and accessible remotely from the alternate work site, such that patches and updates can be applied.

4. Employees shall notify their supervisor and Information Technology Solutions immediately upon the discovery of any inadvertent loss of confidential or sensitive information, or a security incident resulting in the unintentional exposure of University information.

II. Regulatory Compliance

A. The State of Texas has chosen to adopt a select number of Physical and Environmental Protection ("PE") principles established in NIST SP 800-53 "Physical and Environmental Protection" guidelines. The NIST PE controls have been assigned a number; however, the State of Texas has not adopted every NIST PE control, so there are gaps in the numbering sequence. The following subsections outline the PE standards included in TWU's regulations and procedures.

1. PE-1, PE-2, PE-3, PE-6, PE-8, PE-12, PE-13, PE-14, PE-15, PE-16, and PE-17.

III. Compliance

Employees that violate this policy are subject to corrective and disciplinary action, including and up to dismissal, in accordance with TWU's URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes and URP 05.600: Staff Standards of Conduct and Disciplinary Process. TWU may also take corrective action against interns, volunteers, contract Employees, contractors, and/or consultants that violate this policy, including and up to termination of TWU's relations or Access with that individual or entity. Students that violate this policy are subject to corrective and disciplinary action, including and up to suspension or expulsion, in accordance with TWU's URP 06.200: Student Code of Conduct.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

Tex. Admin Code, Ch. 202

Department of Information Resources Security Standards Catalog

NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations

URP 01.320: University Policy Development and Implementation

URP 04.530: Key Control

Office of Human Resources Guide for Exiting Employees

URP 04.705: Information Personnel Security

URP 04.740: Information Security Incident Response

URP 01.310: Records Retention

URP 02.330: Faculty Responsibilities, Standards of Conduct, and Disciplinary Processes

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 05.620: Alternative Work Arrangements for Staff Employees

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

None

Publication Date: **07/02/2021**

Revised: **03/25/2022; 01/08/2024**