Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Physical Access Authorizations**
Regulation and Procedure Number:	**URP: 04.745**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes the information security physical and environmental protection regulations and procedures. The purpose of these regulations and procedures are to mitigate Texas Woman's University's ("TWU") risks from physical security and environmental threats through the establishment of an effective information security physical security and environmental controls program.

APPLICABILITY

This policy is applicable to TWU Students, Employees, 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. "Guests" mean any individual not affiliated with TWU.

3. "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, 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, IR 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.

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

5. "Physically Secured" means locked in a location that denies access to unauthorized personnel. Critical Information Systems include, but not limited to, servers, sans, core routers, and telecommunication switches. Facilities that house critical information systems are generally referred to as server rooms or data centers.

6. "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, and a person who has been admitted or readmitted to TWU.

REGULATION AND PROCEDURE

I. Scope

The scope of these regulations and procedures are 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.

II. Regulations and Procedures

The State of Texas has chosen to adopt the physical and environmental protection principles established in NIST SP 800-53 "Physical and Environmental Protection," Control Family guidelines. The following subsections outline the physical and environmental protection standards that constitute TWU's regulations and procedures.

A. PE-1 Physical and Environmental Protection

1. Regulations

    a. TWU must develop, document, and disseminate physical and environmental protection regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

    a. IT Solutions (“ITS”) will maintain physical and environmental protection regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. PE-2 Physical Access Authorization

1. Regulations

    TWU must:

    a. Develop, approve, and maintain a list of individuals with authorized access to facilities where Information Systems reside;

    b. Issue authorization credentials for facility access;

    c. Review the access list detailing authorized facility access by individuals;

    d. Remove individuals from the facility access list when access is no longer required.

2. Procedures

    a. Facility access is managed using the University card swipe system and centrally managed key program.

    b. System owners shall verify user access lists annually.

C. PE-3 Physical Access Control

1. Regulations

For areas with critical Information Systems TWU must:

    a. Enforce physical access authorization;

    b. Maintain physical access audit logs;

c. Escort and monitor visitors;

d. Change locks or update card swipe systems when keys or cards are lost.

2. Procedures

a. Information Systems are physically secured in an appropriate manner.

b. Non-critical Information Systems are protected by locks that are managed by Facilities Management.

c. Critical Information Systems are protected by card swipe access that are managed by TWU Department of Public Safety (DPS) and Housing.

d. ITS shall escort and/or monitor visitors of critical system facilities.

e. Users must report lost cards or keys to TWU DPS.

D. PE-6 Monitoring Physical Access

1. Regulations

TWU must monitor physical access to facilities where critical information systems reside.

2. Procedures:

Critical Information System facilities entry logs are automatically captured and stored in the University's CBORD system.

E. PE-12 Emergency Lighting:

1. Regulations

TWU must 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. Procedures:

a. ITS critical Information System facilities have battery and gas generators for emergency backup power.

b. ITS critical Information System facilities have emergency that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

F. PE-14 Temperature and Humidity Controls:

1. Regulations:

TWU must maintain and monitor temperature and humidity levels within facilities where critical Information Systems reside.

2. Procedures:

a. TWU Facilities Management maintain, repairs, and monitors the systems that control the temperature and humidity in facilities with critical Information Systems.

b. ITS uses an automated temperature and humidity monitoring systems, alerts are sent to the ITS Information Security. ITS Information Security then notifies the appropriate staff to respond.

G. PE-15 Water Damage Protection:

1. Regulations:

TWU must 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. Procedures:

a. Facilities Management ensures facilities with critical Information Systems have master shutoff or isolation valves that are accessible and are working properly

b. Users must watch an orientation video before receiving access to facilities with critical Information Systems. The orientation video shows users where the water shutoff values are located.

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

Standards of Conduct Corrective Action Guidelines 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 02.330: Faculty Standards of Conduct Corrective Action Guidelines

URP 05.600: Staff Standards of Conduct and Disciplinary Process

URP 06.200: Student Code of Conduct

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 07/02/2021