Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information System Maintenance**
Regulation and Procedure Number:	**URP: 04.785**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This document establishes the Information System maintenance regulations and procedures. The purpose of these regulations and procedures is to manage Texas Woman's University's ("TWU" or "University") risks from Information System maintenance and repairs.

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. "Agency Sensitive Data" applies to less-sensitive business Information that is intended for use within TWU. Its unauthorized disclosure could adversely impact TWU or its Students, strategic partners, and/or Employees.

2. "Confidential Data" applies to the data that is private, confidential by law or otherwise exempt from public disclosure (i.e. exemptions under the Texas Public Information Act, Social Security Numbers, personally identifiable Medical and Medical Payment Information subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. 160, Driver's License Numbers and other government-issued identification numbers,

Education Records subject to the Family Educational Rights & Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), financial account numbers or credit or debit card number in combination with any required security code or Access code permitting Access to an individual's financial account, and/or other University Data about an individual likely to expose the individual to identity theft).

3. "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.

4. "Guests" means any individual not affiliated with TWU.

5. "Information" means data as processed, stored, or transmitted by a computer.

6. "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.

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

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

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

10. “Media” means digital or non-digital storage devices or systems. Digital Media may include, but are not limited to systems, diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives and other portable mass storage devices, compact disks, and digital video disks. Media also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, tablets, and smart phones). Non-digital Media may include but are not limited to paper records/documents or microfilm.

11. "Production System" means a system being used for current operations. A production system is different than a test or development system, which are not used for operational purposes.

12. “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.

13. “System Maintenance” means the various forms of computer or server maintenance needed to keep the Information System running.

14. 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.

15. "User" means an individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules.

REGULATION AND PROCEDURE

I. Security Standards

A. Controlled Maintenance

1. Information System Owners are responsible for ensuring their assigned Information Systems are maintained.

2. The Information System Owner, or designee, shall:

a. Schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on Information System Components in accordance with manufacturer or vendor specifications or University requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Explicitly approve the removal of the Information System or System Components from University facilities for off-site maintenance or repairs;

d. Sanitize equipment to remove all Confidential and Agency Sensitive Data from associated Media prior to removal from University facilities for off-site maintenance or repairs;

e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f. Document maintenance records, including all change management records for maintenance applied to Production Systems.

B. Nonlocal Maintenance

1. TWU authorizes, monitors, and controls any remotely executed (i.e. nonlocal) maintenance and diagnostic activities.

2. The Information System Owner, or designee, shall:

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with University policy and documented in the security plan for the Information System;

c. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

C. Maintenance Personnel

1. Only authorized Employees or University Affiliates shall perform maintenance on TWU Information Resources.

2. The Information System Owner, or designee, shall:

a. Establish a process for maintenance personnel authorization and maintain a list of authorized Users that may perform Information System Maintenance;

b. Ensure that non-escorted personnel performing maintenance on TWU Information Systems have required access authorizations;

c. Escort Guests through sensitive physical security areas; and

d. Designate University personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

II. Regulatory Compliance

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

1. MA-1, MA-2, MA-4, and MA-5.

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 04.730: Information Security Configuration Management

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

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: 03/03/2022