Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Planning**
Regulation and Procedure Number:	**URP: 04.750**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes the information security planning regulations and procedures. The purpose of these regulations and procedures are to manage Texas Woman's University's ("TWU") risks from inadequate security planning through the establishment of an effective security planning program.

APPLICABILITY

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

DEFINITIONS

1. "Authorized Boundary" means all of the components of an information system to be authorized for operation.

2. "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.

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, 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 Security Officer (ISO)" is a designated position required by the State of Texas for each institution of higher education. The ISO is responsible for monitoring the effectiveness of Information Resources security Controls and for administering the Information security program. The designated ISO at TWU is the Director of Technology Infrastructure Director of Enterprise Services and Information Security.

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

7. "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 information security planning principles established in NIST SP 800-53 "Security Planning," Control Family guidelines. The following subsections outline the Security Planning standards that constitute TWU's regulations and procedures.

A. PL-1 Security Planning:

1. Regulations

TWU must develop, adopt, update and review annually, a documented security plan that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

a. As required by TAC 202.71(d)(4), IT Solutions ("ITS") will maintain develop, adopt, update an information security plan.

b. The Information Security Officer ("ISO") will review the information security plan with the Vice President for Finance and Administration annually.

B. PL-2 System Security Plan:

1. Regulations

a. TWU must develop an information security plan that:

i. Is consistent with the organization's enterprise architecture;

ii. Explicitly defines the authorization boundary for the each Information System;

iii. Describes the operational context of the information system in terms of missions and business processes;

iv. Provides the security categorization of the Information System including supporting rationale;

v. Describes the operational environment for the information system and relationships with or connections to other Information Systems;

vi. Provides an overview of the security requirements for the Information System;

vii. Identifies any relevant overlays, if applicable;

viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

x. Is updated to address changes to the Information System/environment of operation or problems identified during plan implementation or security control assessments

b. TWU must securely share the information security plan with appropriate individuals.

2. Procedures:

a. ITS will maintain an information security plan that:

i. Is consistent with the organization's enterprise architecture;

ii. Explicitly defines the authorization boundary for the each information system;

iii. Describes the operational context of the Information System in terms of missions and business processes;

iv. Provides the security categorization of the Information System including supporting rationale;

v. Describes the operational environment for the Information System and relationships with or connections to other Information Systems;

vi. Provides an overview of the security requirements for the Information System;

vii. Identifies any relevant overlays, if applicable;

viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions;

ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; and

x. Is updated to address changes to the Information System/environment of operation or problems

identified during plan implementation or security control assessments.

C. ITS Information Security shares the plan on a secured server with the ISO and Vice President for Finance and Administration.

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