Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Program**
Regulation and Procedure Number:	**URP: 04.755**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes the information security program regulations and procedures. The purpose of these regulations and procedures are to manage Texas Woman's University's ("TWU") risks from compromise of sensitive information due to loss of integrity or confidentiality through the establishment of an information security program.

APPLICABILITY

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

DEFINITIONS

1. "Enterprise Architecture" means the model by which all information systems are implemented into the TWU's environment.

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" is 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.

8. "Threats" means the possible danger that an information system might be attacked or used in an unauthorized manner.

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. Regulation and Procedures

The State of Texas has chosen to adopt the information security program principles established in NIST SP 800-53 "Program Management," Control Family

guidelines. The following subsections outline the information security program standards that constitute TWU's regulations and procedures.

A. PM-1 Information Security Program Plan:

1. Regulations

TWU must develop and disseminate an organization-wide information security program plan that:

a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

c. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical);

d. Is approved by the appropriate person;

e. Is reviewed and updated annually; and

f. Is securely shared with appropriate individuals.

2. Procedures:

IT Solutions ("ITS") maintains TWU's information security program plan that:

a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

b. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

c. Reflects coordination among organizational entities responsible for the different aspects of information security;

d. Is updated annually by the Information Security Officer ("ISO"); and

e. Is approved annually by the Vice President for Finance and Administration.

f. Is securely shared with appropriate individuals.

B. PM-2 Senior Information Security Officer:

1. Regulations

TWU appoints a senior Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

2. Procedures

As required in TAC 202.71(a), the Deputy CIO appoints an Information Security Officer (ISO) and notifies the Texas Department of Information Resources.

C. PM-3 Information Security Resources:

1. Regulations

TWU must ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.

2. Procedures

ITS Information Security performs a risk assessment on all technology purchases. The risk assessment includes recommendations for meeting or enhancing security standards.

D. PM-4 Plan of Action and Milestones Process:

1. Regulations

TWU must implement a process for ensuring that plans of action, including milestones, for the information security program are developed, documented, and executed.

2. Procedures

a. ITS Information Security uses the ITS project management system to record plans of action and includes milestones when appropriate.

b. Plans of action older than 90 days must be reviewed by the ISO.

E. PM-5 Information System Inventory:

1. Regulations

TWU must develop and maintain an inventory of its Information Systems.

2. Procedures

ITS Denton Client Service Manager an inventory of its Information Systems.

F. PM-6 Information Security Measures of Performance:

1. Regulations

TWU must develop and maintain reports on the results of information security measures of performance.

2. Procedures

ITS Information Security develops and maintains reports on the results of information security measures of performance.

G. PM-7 Enterprise Architecture:

1. Regulations

TWU must develop Information Systems architecture with consideration for information security and the resulting risk to TWU operations, assets, individuals, other organizations, and the nation.

2. Procedures

ITS Information Security reviews new Information Systems as needed and critical Information Systems annually to ensure information security architecture is appropriate and up to date.

H. PM-16 Threat Awareness Program:

1. Regulations

TWU must implements an information security threat awareness program.

2. Procedures

ITS Information Security maintains an information security threat awareness program by sending emails, as needed and monthly, on current threats.

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