Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

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

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 and Employees.

DEFINITIONS

1. "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.

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

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. “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 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 Associate Director of 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, or 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.

9. “User” means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Information Security Program Plan

1. 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; and

d. Is approved by the Chancellor and President (“Chancellor”).

2. The Information Security Officer (“ISO”) shall review the information security program plan annually.

3. The information security program plan shall be updated by the ISO as needed to address organizational changes and problems identified during plan implementation or control assessments.

4. The information security program plan shall be protected from unauthorized disclosure and modifications, and securely shared with appropriate individuals.

B. Information Security Program Leadership Role

1. The Deputy CIO shall appoint an Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain a University-wide information security program. The Information Security Officer is charged with the responsibilities enumerated at Texas Government Code § 2054.136 and 1 Texas Administrative Code § 202.21.

2. The Deputy CIO shall notify the Texas Department of Information Resources of the appointment.

C. Information Security and Privacy Resources

1. The Deputy CIO includes the resources needed to implement the information security and privacy programs in capital planning and investment requests and documents all exceptions to this requirement.

2. The ISO and Data Management Officer ("DMO") prepare documentation required for addressing information security (ISO responsibility) and privacy (DMO responsibility) programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards. This information is provided to the Deputy CIO for review.

3. The Deputy CIO makes available for expenditure, where applicable, the planned information security and privacy resources.

D. Plan of Action and Milestones Process

1. The ISO and DMO shall implement a process to ensure that plans of action and milestones for the information security and privacy programs and associated University systems:

a. Are developed and maintained;

b. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to University operations and assets, individuals, other organizations, the State of Texas, and the Nation; and

c. Are reported in accordance with established reporting requirements.

2. The ISO and DMO shall review plans of action and milestones for consistency with the TWU risk management strategy and TWU-wide priorities for risk response actions.

E. Information System Inventory

1. TWU ITS shall develop and maintain an inventory of its Information Systems.

2. The Information System inventory shall be updated annually.

F. Information Security Measures of Performance

1. TWU Information Security and the DMO develop and maintain reports on the results of information security and privacy measures of performance.

G. Enterprise Architecture

1. ITS shall develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to University operations and assets, individuals, other organizations, the State of Texas, and the Nation.

2. TWU Information Security reviews new Information Systems and Critical Information Systems as needed to ensure information security architecture is appropriate and up to date.

H. Risk Management Strategy

1. The ISO and DMO shall develop a comprehensive strategy to manage:

   a. Security risk to University operations and assets, individuals, other organizations, the State of Texas, and the Nation associated with the operation and use of organizational systems; and

   b. Privacy risk to individuals resulting from the authorized processing of personally identifiable information.

2. The ISO and DMO shall implement the risk management strategy consistently across the University.

3. The ISO and DMO shall review and update the risk management strategy as required, to address organizational changes.

I. Authorization Process

The ISO and DMO shall:

1. Manage the security and privacy state of University systems and the environments in which those systems operate through authorization processes;

2. Designate individuals to fulfill specific roles and responsibilities within the University risk management process; and

3. Integrate the authorization processes into a University-wide risk management program.

J. Testing, Training and Monitoring

1. The ISO and DMO shall implement a process for ensuring that University plans for conducting security and privacy testing, training, and monitoring activities associated with University systems:

a. Are developed and maintained; and

b. Continue to be executed.

2. The ISO and DMO shall review testing, training, and monitoring plans for consistency with the TWU risk management strategy and University-wide priorities for risk response actions. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

K. Security and Privacy Groups and Associations

1. TWU Information Security and the DMO shall establish and institutionalize contact with selected groups and associations within the security and privacy communities to:

a. Facilitate ongoing security and privacy education and training for University personnel;

b. Maintain currency with recommended security and privacy practices, techniques, and technologies; and

c. Share current security and privacy information, including threats, vulnerabilities, and incidents.

L. Threat Awareness Program

1. TWU Information Security maintains a threat awareness program that includes a cross-organization information-sharing capability (e.g. email, newsletters, social media) for threat intelligence.

II. Regulatory Compliance

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

1. PM-1, PM-2, PM-3, PM-4, PM-5, PM-6, PM-7, PM-9, PM-10, PM-14, PM-15 and PM-16.

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

Texas Government Code § 2054.133

Texas Government Code § 2054.136

Texas Government Code § 2054.068

URP 01.320: University Policy Development and Implementation

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