Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

This document establishes the information security planning regulations and procedures. The purpose of these regulations and procedures is to manage Texas Woman's University's ("TWU" or "University") risks from inadequate security and privacy planning.

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, and University Affiliates.

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. "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.

4. "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.

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

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

7. "Privacy Officer ("PO") means the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. The designated PO at TWU is the Data Management Officer.

8. "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.

9. "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.

10. "User" means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. System Security and Privacy Plans

1. The ISO is responsible for developing the information security plan. The Privacy Officer ("PO") is responsible for developing the University privacy plan. The information security and privacy plans must:

    a. Be consistent with the University's enterprise architecture;

    b. Explicitly define the constituent Information System Components;

c. Describe the operational context of the Information System in terms of mission and business processes;

d. Identify the individuals that fulfill Information System roles and responsibilities;

e. Identify the information types processed, stored, and transmitted by the Information System;

f. Provide the security categorization of the Information System including supporting rationale;

g. Describe any specific threats to the Information System that are of concern to the organization;

h. Provide the results of a privacy risk assessment for Information Systems processing personally identifiable information;

i. Describe the operational environment for the Information System and any dependencies on or connections to other Information Systems or Information System Components;

j. Provide an overview of the security and privacy requirements for the Information System;

k. Identify any relevant control baselines or overlays, if applicable;

l. Describe the security controls in place or planned for meeting the security and privacy requirements including a rationale for any tailoring and supplementation decisions;

m. Include risk determinations for security and privacy architecture and design decisions;

n. Include security- and privacy-related activities affecting the Information System that require planning and coordination with other TWU officials; and

o. Be reviewed and approved by the Chancellor and President ("Chancellor") or designated representative prior to plan implementation.

2. The security and privacy plans shall be updated to address changes to the Information System or environment of operation or problems identified during plan implementation or security control assessments.

3. The ISO and PO shall securely share copies of the plans and communicate subsequent changes to the plans with appropriate TWU officials.

4. The ISO and PO shall review their respective security and privacy plans annually.

5. The ISO and PO shall protect the plans from unauthorized disclosure and modification.

B. Rules of Behavior

1. TWU shall establish and provide to Users requiring access to TWU Information Resources, the rules that describe their responsibilities and expected behavior for information and Information System usage, security, and privacy (*See* URP 04.700: Computer & Software Acceptable Use Policy).

2. TWU Information Security shall receive a documented acknowledgment from such Users, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the Information System.

3. TWU Information Security requires Users who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually.

4. The Policy Owner reviews and updates URP 04.700: Computer & Software Acceptable Use Policy as needed and in accordance with the policy review timeline.

C. Rules of Behavior | Social Media and External Site/Application Usage Restrictions

1. The rules of behavior shall include restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organizational-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

d. Users are required to follow the social media Community Guidelines (*See* TWU Social Media Community Guidelines), URP 04.700: Computer & Software Acceptable Use Policy,

and URP 04.796: Covered Applications and Prohibited Technology.

D. Baseline Selection

1. The default baseline for TWU Information Systems shall be the Texas Department of Information Resources ("DIR") Security Control Standards Catalog.

2. The Chancellor may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of the University that are more stringent than the standards the Texas DIR prescribes under this section if the more stringent standards:

   a. Contain at least the applicable standards issued by Texas DIR; and/or

   b. Are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the University.

E. Baseline Tailoring

1. TWU may tailor the selected control baseline by applying specified tailoring actions such as applying scoping considerations, selecting compensating controls, assigning values to control parameters, and providing information for control implementation. Tailoring actions facilitate such specialization and customization by allowing the University to develop security and privacy plans that reflect specific mission and business functions, the environments where Information Systems operate, the threats and vulnerabilities that can affect Information Systems, and any other conditions or situations that can impact mission or business success.

2. The Chancellor may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of the University that are more stringent than the standards the Texas DIR prescribes under this section if the more stringent standards:

   a. Contain at least the applicable standards issues by Texas DIR; and/or

   b. Are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best

practices, or deemed necessary to adequately protect the information held by the state agency.

II. Regulatory Compliance

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

1. PL-1, PL-2, PL-4, PL-4(1), PL-10, and PL-11

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

Model Security Plan for Covered Applications and Prohibited Technologies

NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations

Section 2054.133, Government Code

Section 2054.5191, Government Code

TWU Social Media Community Guidelines

URP 01.320: University Policy Development and Implementation

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

URP 04.700: Computer & Software Acceptable Use Policy

URP 04.795 Data Access and Use Policy

URP 04.796: Covered Applications and Prohibited Technology

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; 03/26/2025