Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security and Privacy Awareness and Training**
Regulation and Procedure Number:	**URP: 04.725**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This policy establishes regulations and procedures for both the information security awareness and training program and the privacy awareness and training program The security awareness and training program supports Texas Woman's University's ("TWU" or "University") ability to document, communicate, and train Information Resource Users on security best practices and concepts. The privacy awareness and training program supports educating Information Resource Users on privacy literacy.

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 these regulations and procedures. 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. "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.

2. "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

1

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.

3. "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.

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

5. "Privacy Awareness Training" means a process for educating Users about personal and data privacy literacy.

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

7. "Role-based Security" means a method of regulating access on the basis of the function individual Users provide within the organization.

8. "Security Awareness Training" means a process for educating Users about information and computer security.

9. "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.

10. "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.

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

REGULATION AND PROCEDURE

I. Security Standards

   A. Literacy Training and Awareness

      1. Security Awareness Training

         a. IT Solutions ("ITS") implements and maintains Security Awareness Training for all Information Resource Users

required by the state as part of initial training for new Users or when required by Information System changes.

b. State-required Information Resource Users at TWU must complete and pass Security Awareness Training upon assignment to TWU and a refresher course annually.

c. The ISO and the TWU Information Security team shall maintain, manage, review, and update Security Awareness Training as needed and as changes are made to systems, policies, and regulations to ensure that the most recent security practices are being used and distributed via the training.

d. ITS shall introduce information security awareness and inform new Employees of Security Awareness Training and policies and procedures via new employee orientation.

e. ITS shall provide an ongoing information security awareness education program for all Users.

2. Privacy Awareness Training

a. The TWU Privacy Officer implements and maintains Privacy Awareness Training.

b. Privacy Awareness Training is provided to all Information Resource Users upon assignment to TWU. Users shall complete a refresher course annually.

c. The Privacy Officer shall maintain, manage, review, and update Privacy Awareness Training as needed and as changes are made to systems, policies, and regulations to ensure that the most recent privacy practices are being used and distributed via the training.

d. The Privacy Officer shall introduce privacy awareness and inform new employees of privacy training, policies and procedures via new employee orientation.

3. To increase the security and privacy awareness of system Users, ITS and the TWU Privacy Officer shall employ techniques including, but not limited to, generating notices and email advisories, conducting awareness events, and displaying information security and privacy awareness signage.

4. TWU shall incorporate lessons learned from internal and external security or privacy incidents or breaches into security and privacy literacy training and awareness techniques.

B. Insider Threat

1. TWU Security Awareness Training shall include content educating Users to recognize and report potential indicators of insider threats.

C. Role-Based Training

1. TWU shall provide role-based security and privacy training to Users with information security or privacy responsibilities. Training shall be provided prior to the User performing assigned duties.

2. Users that are assigned a role-based training shall complete the training within 30 days of assignment and complete a refresher course as assigned (frequency is dependent on the specific training) or when required by Information System changes.

3. TWU shall incorporate lessons learned from internal and external security or privacy incidents or breaches into role-based training.

D. Training Records

1. ITS maintains records of Security Awareness Training and monitors User records for compliance. These records are retained in accordance with TWU's Records Retention policy.

2. The Privacy Officer maintains records of Privacy Awareness Training and monitors User records for compliance. These records are retained in accordance with TWU's Records Retention policy.

3. Regulation-specific Information System security or privacy training activities or specific Information System security or privacy training shall be maintained and retained by the appropriate business functional area.

II. Regulatory Compliance

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

1. AT-1, AT-2, AT-2(2), AT-3, and AT-4.

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

Texas Government Code § 2054.519

Texas Government Code § 2054.5191

Texas Government Code § 2054.5192

Department of Information Resources Security Control 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 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

URP 01.310: Records Retention

FORMS AND TOOLS

None