

Texas Woman's University University Regulation and Procedure

Regulation and Procedure Name: Information Security Awareness Training

**Regulation and Procedure
Number: URP: 04.725**

Policy Owner: Finance and Administration

POLICY STATEMENT

This policy establishes the information security awareness training regulations and procedures. The security awareness and education program helps Texas Woman's University ("TWU") document, communicate, and train information resource users on security best practices and concepts.

APPLICABILITY

This policy is applicable to TWU Students, Employees, and University Affiliates.

DEFINITIONS

1. "Client-Services" means OOT staff members employed as part of Client Services to perform the first line of support to TWU for technology-related incidents and service requests.
2. "Developer is an Office of Technology in IT Solutions (ITS)" means a staff member who creates software and is employed as part of Enterprise Applications.
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, 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, IR 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. "Infrastructure" means an OOT staff member employed as part of Technology Infrastructure to create and maintain a collection of physical and/or virtual resources that support an overall technology environment: server, storage, and network components.
8. "Role-based Security" means a method of regulating access on the basis of the function individual users provide within an enterprise.
9. "Security Awareness Training" means a process for educating employees about information and computer security.
10. "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.
11. "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.

12. "User" means TWU Employees, contractors, vendors, or other people using a TWU information resource.

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 Security and Awareness principles established in NIST SP 800-16 "Information Technology Security Training Requirements: A Role-Based and Performance-Based Model." The following subsections outline the security and awareness standards that constitute TWU regulations and procedures.

A. AT-1 Security Awareness and Training

1. Regulations

TWU must develop, adopt or adhere to a formal, documented security awareness and training regulations and procedures that addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance.

2. Procedures

IT Solutions (“ITS”) will maintain regulations and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational units, and compliance of TWU’s security awareness and training program.

B. AT-2 Security Awareness Training

1. Regulations

TWU must provide basic Security Awareness Training to all Information Resource users as part of initial training for new users, when required by Information System changes, and annually thereafter.

2. Procedures

- a. ITS implements and maintains Security Awareness Training for all Information Resource users to help ensure an understanding of computer security related issues.
- b. Information Resource users at Texas Woman’s University must complete and pass a basic security awareness course upon assignment to TWU and an annual refresher course annually.
- c. ITS utilizes several learning management platforms to offer security training, all of which are subject to change based on the budget and needs of the University.
- d. It is the responsibility of the Information Security Officer (“ISO”), and the Information Security team to maintain, manage, review, and update the security awareness training(s) as needed to ensure the most recent security practices are being used and distributed.
- e. New employee orientation is also used to introduce information security awareness and inform new employees of information security policies and procedures.
- f. ITS Information Security will maintain a monthly university wide e-mail newsletter informing users of recent information security news and trends.

C. AT-3 Role-Based Security Training

1. Regulations

TWU must provide Role-based Security-related training as part of initial training for new users and when required by Information System changes.

2. Procedures

a. Role-based Security training will be provided to staff with information security responsibilities; this includes all of ITS and will be broken into three separate role-based training as follows.

i. Developer, will take a “Developer Security Awareness Training” consisting of a mixture of general information security practices and work specific security issues such as coding practices and web application vulnerability.

ii. Infrastructure, will take an “Infrastructure Security Awareness Training” consisting of a mixture of general information security practices and work specific security issues such as information system access and encryption.

iii. Client-Services, will take a “Client Services Security Awareness Training” consisting of a mixture of general information security practices and work specific security issues such as client identity verification and sensitive information disposal.

b. Just as with the basic security awareness training TWU utilizes several platforms that can be used to provide web based training, all of which are subject to change based on the budget and needs of the University.

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: 10/08/2021