Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Assessment, Authorization, and Monitoring**
Regulation and Procedure Number:	**URP: 04.715**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This document establishes information security assessment, authorization, and monitoring regulations and procedures. The purpose of these regulations and procedures is to manage risks that may impact Texas Woman's University ("TWU" or "University") from inadequate security assessment, authorization, and continuous monitoring of university information assets.

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. "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 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. "Information System Owner" means the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an Information System.

6. "Security Assessment" means an explicit study to locate Information Systems security vulnerabilities and risks.

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. "System Interconnections" are the direct connections of two or more information systems.

9. "Third-party" means a person who is not paid through TWU's payroll system or an organization that is not directly governed by TWU's Board of Regents.

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:

1. 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.

2. Employee of a Governmental Agency: an individual employed by a federal or Texas state agency.

3. Employee of a TWU-Affiliated Institution: an individual who works for organizations that are tightly aligned with the University.

4. Pre-Employment Individual: an individual who will be hired by the University and the hiring department has sponsored their access to TWU resources.

5. 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. Control Assessments

1. TWU IT Solutions ("ITS") shall develop a control assessment plan that describes the scope of the assessment including:

a. Security controls and control enhancements under assessment;

b. Assessment procedures to be used to determine control effectiveness; and

c. Assessment environment, assessment team, and assessment roles and responsibilities.

2. ITS shall ensure that the control assessment plan is reviewed and approved by the ISO, or designee, prior to conducting the assessment.

3. The control assessment shall assess and review the University security controls in relation to the Security Controls Catalog and the environment of operation biennially to determine the

extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the University's security requirements.

4. The control assessment shall produce a control assessment report that documents the results of the assessment.

5. The ISO, or designee, shall provide the results of the control assessment to the Chief Information Officer or other designated representative.

6. The control assessment shall be performed by an independent Third-party.

B. Information Exchange

1. TWU Information Systems that have connections from an Information Resource to other Information Systems outside of an authorization boundary must be authorized through the use of contracts, interconnection security agreements, memoranda of understanding or agreement, service level agreements, User agreements, or nondisclosure agreements.

2. Each interconnection or exchange agreement shall document the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated.

3. Users shall request system interconnections and exchanges via the Service Request System. The request should document contact information, purpose of connection, scope of needs, Third-party information, connection use, redundant connections, approximate connection duration, possible exchange or interconnection agreements, and any other pertinent information. The Information System Owner, or designee, shall approve and document the request.

4. The Information System Owner, or designee, involved in the interconnection shall manage, review and update the exchange agreements on an as-needed basis to verify enforcement of security requirements.

C. Plan of Action and Milestones

1. TWU Information Security will develop a plan of action and milestones to document TWU's planned remediation actions to correct weaknesses or deficiencies noted during the assessment of

the controls and to reduce or eliminate known vulnerabilities in the system.

2. The ISO shall update the existing plan of action and milestones periodically, and biennially at minimum, based on the findings from control assessments, audits, and continuous monitoring activities.

D. Security Authorization

1. TWU Information Security shall identify an Information System Owner for each Information System. The Information System Owner will be identified on the Service Evaluation & Risk Assessment form.

2. The ISO is the designated authorizing official for common controls available for inheritance by TWU systems.

3. The Information System Owner shall sign the Service Evaluation & Risk Assessment form after the risk assessment has been conducted. The signature constitutes:

   a. Their authorization to commence operations of the Information System; and

   b. Acceptance of the use of common controls inherited by the Information System.

4. The ISO shall sign the Service Evaluation & Risk Assessment form and authorize the use of common controls for inheritance by TWU systems.

5. If applicable, Data Owners as defined in URP 04.795: Data Access and Use Policy shall also sign the Service Evaluation & Risk Assessment form and authorize the data use detailed in the risk assessment.

6. Authorizations shall be updated as necessary and upon changes to Information System Owner personnel. Business functional units shall notify TWU Information Security of changes to Information System Owners.

E. Continuous Monitoring

1. TWU Information Security, in consultation with Information System Owners, shall develop a continuous monitoring strategy and implement a continuous monitoring strategy that includes:

a. Establishment of system-level metrics to be monitored;

b. Establishment of monitoring frequency and frequencies for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and TWU-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to the Chief Information Officer or other designated personnel.

F. Continuous Monitoring | Risk Monitoring

1. The ISO shall ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;

b. Compliance monitoring; and

c. Change monitoring.

G. Penetration Testing

1. TWU Information Security shall conduct penetration testing biennially.

2. Penetration test scopes are defined per test to meet organization needs.

3. TWU Information Security shall coordinate with appropriate personnel and Information System Owners regarding penetration test results and address vulnerabilities identified in the test.

H. Internal System Connections

The Information System Owner, or designee, shall:

1. Authorize internal connections for the following class of Information System Components with common characteristics

and/or configurations: workstations, servers, network equipment, printers, scanners, and copiers;

2. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

3. Terminate internal system connections upon service deprecation; and

4. Review the continued need for each internal connection on an as-needed basis.

II. Regulatory Compliance

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

1. CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-7 (4), CA-8, and CA-9.

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 § 2054.516(a)(2)

Department of Information Resources Security 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 04.795: Data Access and Use Policy

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

Service Evaluation & Risk Assessment Form

Service Request System

Publication Date: 07/02/2021

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