Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

This document establishes information security assessment and authorization regulations and procedures. The purpose of these regulations and procedures are to manage risks that may impact Texas Woman's University ("TWU") from inadequate security assessment, authorization, and continuous monitoring of university information assets through the establishment of an effective security planning program.

APPLICABILITY

This policy is applicable to TWU Students, Employees, and Guests.

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. "Guests" means any individual not affiliated with TWU.

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, 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 Director of Technology Infrastructure Director of Enterprise Services and 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. "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, and 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.

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 Assessment and Authorization principles established in NIST SP 800-53 "Security Assessment and

Authorization," Control Family guidelines. The following subsections outline the information security assessment and authorization standards that constitute TWU regulations and procedures.

A. CA-1 Security Assessment and Authorization:

1. Regulations

TWU must develop, adopt or adhere to a formal, documented security assessment and authorization procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

IT Solutions ("ITS") will maintain regulations and procedures for assessment and authorization that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. CA-2 Security Assessments:

1. Regulations

TWU must:

a. Develop a security assessment plan that describes the scope of the assessment that includes:

i. Security controls and control enhancement under assessment.

ii. Assessment procedure to be used to determine security control effectiveness.

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

b. Assess the security controls in the information asset on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Information System.

c. Produce a Security Assessment report that documents the results of the assessment.

d. Provide the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

2. Procedures

a. ITS Information Security will contract a Third Party to perform external penetration testing on all of TWU's critical information systems on an annual basis.

b. ITS Information Security will contract a Third Party to perform an assessment of internal security controls on an annual basis.

c. ITS Information Security will use the penetration test results to assess the effectiveness of security regulations and procedures and will suggest changes that they feel are required.

d. ITS Information Security will share the results of the Third Party assessments, as well as their own findings to the ISO.

C. CA-3 System Interconnections:

1. Regulations

a. TWU Information Systems that have connections from the information asset to other Information Systems outside of the authorization boundary must be authorized through the use of Interconnection Security Agreements.

b. TWU must monitor information assets connections on an ongoing basis verifying enforcement of security requirements.

2. Procedures

a. Requests for system interconnections must be submitted through the Service Request System, approved and documented. The request should document contact information, purpose of connection, scope of needs, Third Party information, connection use, redundant connections, approximate connection duration, Possible Standard Non-Disclosure Agreements, and other useful information.

b. The Information Security Manager will monitor Third Party connections to ensure security requirements are maintained.

D. CA-5 Plan of Action and Milestones

1. Regulations

TWU must develop and update a plan of action and milestones for the Information System to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.

2. Procedures

ITS Information Security will develop and maintain a plan of action for remedial actions to correct deficiencies noted during the assessment of the security controls.

E. CA-6 Security Authorization:

1. Regulations

TWU must:

a. Identify an owner for each Information System.

b. Ensure that the owner authorizes the Information System for processing before commencing operations.

2. Procedures

a. ITS Information Security will identify the executive owner on the Risk Assessment form.

b. The risk assessment signature from the Information System owner constitutes their authorization to commence operations of the information system.

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

Risk Assessment Form

Publication Date: 07/02/2021

Revised: 07/02/2021