Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Risk Assessment**
Regulation and Procedure Number:	**URP: 04.760**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document establishes the information security risk assessment regulations and procedures, for managing risk associated with information assets, information leakage, and network vulnerabilities. The information security risk assessment regulations and procedures proactively identifying threats and vulnerabilities, which can result in consequences to Texas Woman's University ("TWU").

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 these regulations and procedures. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

APPLICABILITY

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

DEFINITIONS

1. "Data Owner" is an individual who can authorize or deny Access to certain data, and who is responsible for that data's accuracy, integrity, and timeliness.

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

4. "Information" means data as processed, stored, or transmitted by a computer.

5. “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.

6. “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.

7. “Information System” is a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

8. “Risk Assessment” means an objective analysis of the effectiveness of security controls that protect an organization’s assets and a determination of the probability of losses to those assets.

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, and a person who has been admitted or readmitted to TWU.

10. “Vulnerability Scanner” means a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

REGULATION AND PROCEDURE

I. Policy

The State of Texas has chosen to adopt the risk assessment principles established in NIST SP 800-53 “Risk Assessment,” Control Family guidelines. The following subsections outline the risk assessment standards that constitute TWU’s regulations and procedures.

II. Regulation and Procedure

A. RA-1 Risk Assessment Regulations

1. Regulations

TWU must develop, adopt, or adhere to, formal documented risk assessment regulations and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Procedures

IT Solutions (“ITS”) will maintain regulations and procedures for risk assessments that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. RA-2 Security Categorization:

1. Regulations

TWU must:

a. Categorize Information Systems and the data stored within these systems, in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance;

b. Document the security categorization in the security plan for the Information Systems; and

c. Ensure that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

2. Procedures

a. ITS Information Security categorizes Information Systems and Information and seeks category owner authorizing official designated representative on the Risk Assessment form.

b. ITS Information Security defines categories within the information security plan.

c. ITS Information Security categorizes Information Systems in the information security plan.

C. RA-3 Risk Assessments:

1. Regulations

TWU must:

a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the data the system processes, stores, or transmits;

b. Document Risk Assessment results in a risk assessment report;

c. Review Risk Assessment results of critical information systems;

d. Disseminate Risk Assessment results to appropriate authorizing officials; and

e. Update the Risk Assessment whenever there are significant changes to the Information System or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

2. Procedures

a. ITS Information Security conducts Risk Assessments on all new Information Systems.

b. ITS Information Security documents the Risk Assessment using the ITS Risk Assessment form.

c. ITS Information Security ensures appropriate system/Data Owner(s) (i.e., authorizing officials) accept the risk noted on

the Risk Assessments before Information Systems are put into production (i.e., begin to be used by the University).

d. Each year, ITS Information Security completes a Risk Assessment of critical Information Systems.

e. The Information Security Officer ("ISO") may ask ITS Information Security to complete a Risk Assessment of any Information System when the ISO deems it necessary.

D. RA-5 Vulnerability Scanning:

1. Regulations

TWU shall:

a. Perform periodic network scans for vulnerabilities in the Information System and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

i. Enumerating platforms, software flaws, and improper configurations;

ii. Measuring the criticality and impact of the vulnerability;

iii. Providing checklists, remediation steps and validation procedures;

iv. Providing departmental or role based access to remediate respective findings, and

v. Tracking historical vulnerability discovery and remediation efforts.

c. Analyze vulnerability scan reports and results from security control assessments;

d. Remediate vulnerabilities in a timely manner commensurate with the criticality and exposure of security risk to the institution; and

e. Ensure asset, system, or application owners coordinate with ITS staff to identify and minimize the likelihood and impact of vulnerabilities.

III. Compliance

A. Unless coordinated with the TWU Information Security Officer, unpatched or un-remediated systems will be quarantined and disconnected from the TWU network after the timeframe for remediation has expired.

B. 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 URP 02.330: Faculty Ethics, Standards of Conduct and Disciplinary Process 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

ITS Risk Assessment Form

Publication Date: 07/02/2021

Revised: 07/02/2021