Texas Woman's University
University Regulation and Procedure

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

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 seeks to proactively identify threats and vulnerabilities, which can result in consequences to Texas Woman's University ("TWU" or "University").

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 Employees and University Affiliates.

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

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, 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.

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 Associate Director of Information Security.

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

7. “Information System Component” means a discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an Information System.

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. “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.

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

11. "Vulnerability Scanner" means a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

REGULATION AND PROCEDURE

I. Security Standards

A. Security Categorization

1. TWU Information Security categorizes Information Systems and the Information the systems process, store, and transmit via the risk assessment process.

2. The Service Evaluation & Risk Assessment Form documents the security categorization results, including supporting rationale, in the security plan for the system.

3. TWU Information Security verifies that the authorizing official or authorizing official designated representative (Information System Owner or designee and appropriate Data Owner, if applicable) reviews and approves the security categorization decision.

B. Risk Assessments

TWU Information Security shall:

1. Conduct a Risk Assessment, including:

    a. Identifying threats to and vulnerabilities in the Information System;

    b. Determining 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; and

    c. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

2. Perform Risk Assessments on all new Information Systems;

3. Integrate organizational Risk Assessment results (such as those performed by the Office of Audit Services) and risk management decisions from the University and mission or business process perspectives with Information System-level Risk Assessments;

4. Document Risk Assessment results via the Risk Assessment Service Request ;

5. Ensure appropriate Information System Owner and, where appropriate, Data Owner(s) (i.e., authorizing officials), accept the risk noted on the Risk Assessment before Information Systems are put into production (i.e., begin to be used by the University);

6. Disseminate Risk Assessment results to appropriate authorizing officials;

7. Review Risk Assessment results and complete a new Risk Assessment in line with the criteria for reassessment documented in the Information System's Risk Assessment report; and

8. Update the Risk Assessment when 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 or privacy state of the system.

9. The Information Security Officer (“ISO”) may ask TWU Information Security to complete a Risk Assessment of any Information System when the ISO deems it necessary.

C. Supply Chain Risk Assessment

TWU Information Security shall:

1. Assess supply chain risks associated with Information Systems; and

2. Update the supply chain Risk Assessment periodically and when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

D. Vulnerability Monitoring and Scanning

TWU Information Security shall:

1. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned;

2. Monitor and scan for vulnerabilities in the system and hosted applications on a regular basis and when new vulnerabilities potentially affecting the system or applications are identified and reported;

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

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

   b. Measuring the criticality and impact of the vulnerability;

   c. Providing checklists, remediation steps and validation procedures; and

   d. Providing departmental or role-based access to remediate respective findings.

4. Analyze vulnerability scan reports and results from vulnerability monitoring;

5. Remediate legitimate vulnerabilities in a timely manner commensurate with the criticality and exposure of security risk to the

University (see Information Security Standard - Vulnerability Remediation);

6. Share information obtained from the vulnerability monitoring process and assessments with applicable personnel to help eliminate similar vulnerabilities in other systems; and

7. Ensure Information Resource, Information System, or application owners coordinate with ITS staff to identify and minimize the likelihood and impact of vulnerabilities.

E. Vulnerability Monitoring and Scanning | Update Vulnerabilities To Be Scanned

Vulnerabilities to be scanned are updated prior to a new scan and when new vulnerabilities are identified and reported.

F. Vulnerability Monitoring and Scanning | Public Disclosure Program

TWU Information Security shall establish a public reporting channel for receiving reports of vulnerabilities in Information Systems and Information System Components (*See* Public Disclosure Program under Forms and Tools section of this URP).

G. Risk Response

1. TWU ITS shall respond to findings from security and privacy assessments, monitoring, and audits in proportion with University risk.

II. Regulatory Compliance

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

1. RA-1, RA-2, RA-3, RA-3(1), RA-5, RA-5(2), RA-5(11), and RA-7.

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 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.

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 Data Classification Guide

Department of Information Resources Security Standards Catalog

Information Security Standard - Vulnerability Remediation

NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations

Section 2054.077, Texas Government Code

Section 2058.077, Texas Government Code

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

FORMS AND TOOLS

Public Disclosure Program

Risk Assessment Service Request

Publication Date: 07/02/2021

Revised: 03/25/2022; 03/26/2025