Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**System and Information Integrity**
Regulation and Procedure Number:	**URP: 04.780**
Policy Owner:	**Finance and Administration and Information Technology Solutions**

POLICY STATEMENT

This document establishes the system and information integrity regulations and procedures. The purpose of these regulations and procedures is to manage Texas Woman's University's ("TWU") risks from Information System flaws and vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. The integrity of data, its source, its destination, and processes applied to it shall be assured, and changes to data shall be made only in an authorized manner.

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

3. "Information Security Officer ("ISO")" means 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 Resource” 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 System” means a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

6. “Information System Integrity” means the assurance that the information is trustworthy and accurate, and functioning in an operating system environment that is free of software conflicts.

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

8. “Malicious Code” means any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to an Information System.

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

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:

    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.

11. “User” means an individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner’s procedures and rules.

REGULATION AND PROCEDURE

I. Security Standards

A. Flaw Remediation

1. TWU Information Security shall monitor and use Information gathering systems to identify, track, report, and help correct any potential system flaws that may hinder Information or Information System Integrity.

2. Information System Owners shall test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

3. All Information Systems must be configured using the Configuration Management Process document. Different monitoring

and reporting methods or standards are utilized depending on system setup, use, and information accessed. Information Systems that are not set up to auto-update are the responsibility of the Information System Owner to maintain and update.

4. Information System Owners must review infrastructure patches on a regular basis (*See* Vulnerability Remediation Information Security Standard) and work with appropriate system users to coordinate applying the patches.

5. Information Systems patched by TWU are scanned by TWU Information Security with vulnerability scanning software upon creation and are subject to additional scans for security flaws. Information Systems containing or accessing sensitive information are scheduled to be scanned at regular intervals. Vulnerabilities are reported to the system administrator and TWU Information Security to ensure steps are taken to remedy any potential vulnerabilities.

B. Malicious Code Protection

1. IT Solutions ("ITS") shall use various tools, systems and techniques to protect against Malicious Code. These mechanisms shall be employed at Information System entry and exit points to detect and eradicate malicious code.

2. ITS Malicious Code protection tools and systems must be kept updated to configuration management standards.

3. ITS Malicious Code protection systems perform periodic scans and real-time scans of files from external sources. External sources are real-time scanned when they are delivered through TWU's email system or as the files are downloaded, opened, or executed.

4. ITS Malicious Code protection systems block or quarantine malicious code and send alerts to TWU Information Security to assess the potential risk, false positive detection, eradication, and the resulting potential impact on the availability of the Information System.

C. Information System Monitoring

1. ITS shall monitor Information Systems to detect attacks, indicators of potential attacks, unauthorized local, network, and remote connections on the basis of TWU's needs and service offerings.

2. ITS identifies unauthorized use of the Information System through the use of various tools, systems, and techniques.

3. ITS utilizes monitoring devices at strategic points within the Information System.

4. Information System Owners shall ensure that Information System logs are enabled, secured, and retained.

5. Only authorized Users shall have access to or modify Information System logs.

6. ITS heightens the level of Information System monitoring activity whenever there is an indication of increased risk to TWU operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

7. Where applicable, the Deputy Chief Information Officer and ISO shall consult with TWU's Office of General Counsel with regard to Information System monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

8. When the ISO receives credible information on an increased risk to information security, they shall notify TWU Information Security to deploy additional manual interventions as necessary to meet the new risk.

D. Security Alerts, Advisories, and Directives

1. TWU Information Security and ISO receive security notices, alerts, and other useful information from the Texas Department of Information Resources.

2. ITS utilizes various tools, systems and techniques to generate internal security alerts, advisories, and directives. These

communications are disseminated, as necessary, to Information System Owners or Users.

3. TWU Information Security reports security incidents and statistical information to the State of Texas on a monthly basis. Information for these reports are gathered from several internal systems, ticketing systems, network security appliances, and networked antivirus reporting and management interfaces.

4. Information System Owners are notified of security related issues or noncompliance through automated monitoring and reporting systems or directly by TWU Information Security.

E. Information Input Validation

The Information System Owner, or designee, shall check the validity of inputs to Information Systems. Inputs may include, but are not limited to, character set, length, numerical range, and acceptable values.

F. Information Management and Retention

TWU handles and retains output from the Information System in accordance with applicable laws, standards, and operational requirements. The Information System Owner, or designee, is responsible for handling and retaining Information according to the requirements of the TWU record retention schedule.

II. Regulatory Compliance

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

1. SI-1, SI-2, SI-3, SI-4, SI-5, SI-10, and SI-12.

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

1 Tex. Admin. Code Ch. 203

13 Tex. Admin. Code Ch. 613

Department of Information Resources Security Standards Catalog

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

Retention Schedules for Texas State Agencies and Public Universities

Texas Business and Commerce Code § 512.053

Texas Government Code § 441.185

URP 01.320: University Policy Development and Implementation

URP 04.730: Information Security Configuration Management

URP 04.760: Information Security Risk Assessment

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

URP 01.310 Records Retention

Information Security Standard - Vulnerability Remediation

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 03/03/2022; 02/28/2024