Texas Woman's University
University Regulation and Procedure

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

POLICY STATEMENT

This document establishes the information integrity regulations and procedures. The purpose of these regulations and procedures are to manage Texas Woman's University's ("TWU") risks from information system flaws/vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling through the establishment of an information integrity 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 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 Director of Technology Infrastructure Director of Enterprise Services and 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 Integrity" means the assurance that the information is trustworthy and accurate, and functioning in an operating system environment that is free of software conflicts.

6. “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.

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.

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 Access Control principles established in NIST SP 800-53 “System and Information Integrity,” Control Family guidelines. The following subsections outline the system and information integrity standards that constitute TWU’s regulations and procedures.

A. SI-1 System and Information Integrity

1. Regulations:

TWU must develop, adopt, or adhere to a formal, documented Information System integrity regulations and procedures 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 Information System integrity regulations and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

B. SI-2 Flaw Remediation

1. Regulations:

a. TWU must:

i. Identify, report, and correct information system flaws;

ii. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

iii. Install security-relevant software and firmware updates on a regular basis or when the Information Security Officer (“ISO”) deems necessary; and

iv. Incorporates flaw remediation into the University's configuration management process.

2. Procedures

a. ITS Information Security utilizes monitoring and information gathering systems to identify, track, report, and help correct any potential systems flaws that may hinder system or information integrity.

b. All Information Systems must be configured using the Operating System Configuration Guidelines 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 system owner to maintain and update.

c. Critical Information Systems owners must review infrastructure patches on a monthly basis and work with appropriate system users to coordinate applying the patches.

d. All Information Systems are scanned by ITS 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 ITS Information Security to ensure steps are taken to remedy any potential vulnerabilities.

C. SI-3 Malicious Code Protection

1. Regulations:

a. TWU must:

i. Employ Malicious Code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

ii. Update Malicious Code protection mechanisms whenever new releases are available; and

iii. Configure Malicious Code protection mechanisms to:

iv. Perform periodic scans of the Information Systems and real-time scans of files from external sources when delivered through email or as the files are downloaded, opened, or executed in accordance with organizational security policy;

v. Block Malicious Code; quarantine Malicious Code; send alert to appropriate personnel; and

vi. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

2. Procedures:

a. ITS utilizes various tools, systems and techniques to protect against malicious code, these services are subject to change on the basis of TWU's needs, and service offerings.

b. 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.

c. ITS Malicious Code protection systems block or quarantine malicious code and send alerts to ITS Information Security to assess the potential risk and/or false positive detection.

D. SI-4 Information System Monitoring

1. Regulations:

a. TWU must:

i. 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;

ii. Attempt to identify unauthorized use of the Information Systems;

iii. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

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

v. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

2. Procedures:

a. ITS utilizes various tools, systems and techniques to monitor possible security related issues, these services are subject to change on the basis of TWU's needs, and service offerings.

b. ITS Information Security ensures that Information System monitoring logs are secured and retained.

c. The Deputy Chief Information Officer and ISO consult with TWU's General Counsel before ITS deploys a new Information System monitoring technique.

d. When the ISO receive credible information on an increased risk to information security, they notify ITS Information Security to deploy additional manual interventions as necessary to meet the new risk.

E. SI-5 Security Alerts, Advisories, and Directives:

1. Regulations:

a. TWU must

i. Receive information system security alerts, advisories, and directives from the Texas Department of Information Resources on an ongoing basis;

ii. Generate internal security alerts, advisories, and directives as deemed necessary;

iii. Disseminate security alerts, advisories, and directives to Information System owners; and

iv. Implement security directives in accordance with established time frames, or notifies the issuing information system owner of the degree of noncompliance.

2. Procedures:

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

b. ITS utilizes various tools, systems and techniques to alert Information System owners of possible security related issues, these services are subject to change on the basis of TWU's needs, and service offerings.

c. ITS 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.

d. Information System owners are notified of security related issues through automated monitoring and reporting systems or directly by ITS Information Security.

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

None

Publication Date:	**07/02/2021**
Revised:	**07/02/2021**