Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information Security Incident Response**
Regulation and Procedure Number:	**URP: 04.740**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This document serves to establish information security incident response regulations and procedures. The purpose of these regulations and procedures are to improve Texas Woman's University's ("TWU") capability to identify, respond, and manage information security incidents, which may occur across the university environment.

APPLICABILITY

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

DEFINITIONS

1. "Cyber Forensics" means is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

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. "Security Incident" means the act of violating an explicit or implied security regulation. Incidents include but are not limited to:

    a. attempts (either failed or successful) to gain unauthorized access to an information system or its data

    b. unwanted disruption or denial of service

c. the unauthorized use of an information system for the processing or storage of data

d. changes to information system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

5. “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 incident management principles established in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-61 “Computer Security Incident Handling Guide”. The following subsections outline the incident management standards that constitute TWU’s regulations and procedures.

A. IR-1 Incident Response

1. Regulations

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

B. IR-4 Incident Handling

1. Regulations

TWU must develop, adhere to or adopt incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

2. Procedures

a. ITS maintains a document entitled “Texas Woman’s University Incident Response Plan” (“TWUIRP”) which outlines the reporting, escalation, handling, and documentation of incidents. The TWUIRP is updated with new information and processes based on testing, usage, and feedback.

b. ITS Information Security also reports all incident data on a monthly basis to the Texas Department of Information Resources (“DIR”) through the online DIR Archer reporting system.

C. IR-5 Incident Monitoring

1. Regulations

TWU must develop, adhere to or adopt incident monitoring processes which track and document information asset security incidents on an ongoing basis.

2. Procedures

ITS Information Security tracks and records security incidents using several methods including but not limited to incidents reported through, the service request system, antivirus systems, and network security systems.

D. IR-6 Incident Reporting

1. Regulations

Users that discover a suspected security incident must report the incident immediately.

2. Procedures

All information system users must report a suspected security incident to the Service Desk by phone 940-898-3971, email servicedesk@twu.edu, or service request system.

E. IR-8 Incident Response Plan

1. Regulations

a. TWU must develop an incident response plan that:

i. Provides the university with a roadmap for implementing its incident response capability;

ii. Describes the structure and organization of the incident response capability;

iii. Provides a high-level approach for how the incident response capability fits into the overall university;

iv. Meets the unique requirements of the university, which relate to mission, size, structure, and functions;

v. Defines reportable incidents;

vi. Provides metrics for measuring the incident response capability within the university;

vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

viii. Is reviewed, updated, approved and securely communicated to the appropriate individuals.

2. Procedures

a. OOT maintains an TWUIRP that:

i. Provides the university with a roadmap for implementing its incident response capability;

ii. Describes the structure and organization of the incident response capability;

iii. Provides a high-level approach for how the incident response capability fits into the overall university;

iv. Meets the unique requirements of the university, which relate to mission, size, structure, and functions;

v. Defines reportable incidents;

vi. Provides metrics for measuring the incident response capability within the university;

vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability.

b. ITS TWUIRP is created, maintained and tested by the OOT Security Team annually.

c. ITS TWUIRP is reviewed and updated by the Information Security Officer ("ISO") annually.

d. ITS TWUIRP is approved by the Vice President for Finance and Administration annually.

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 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

DIR Archer Reporting System

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