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 and Information Technology Solutions**

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" or "University") capability to identify, respond, and manage information security incidents, which may occur across the university environment.

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. "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 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.

3. “Information Spillage” means instances where information is placed on Information Systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to an Information System and subsequently is determined to be of a higher classification or impact level.

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

6. “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

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.

8. “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.

9. “User” means TWU Employees, contractors, vendors, or other people using a TWU Information Resource.

REGULATION AND PROCEDURE

I. Security Standards

A. Incident Response Training

1. IT Solutions (“ITS”) implements and maintains Incident Response training for assigned Users with information security incident roles and responsibilities.

2. Assigned Users shall complete Incident Response training within 30 days of their assigned Incident Response role, with respect to changes in the Information System, and complete a refresher course annually thereafter.

3. Incident Response training content shall be updated periodically and following significant changes to the Information System.

B. Incident Response Testing

The effectiveness of the Incident Response capability for the Information System shall be tested annually using tabletop exercises, simulations, or real-world incident response circumstances.

C. Incident Handling

1. ITS maintains a document entitled “Texas Woman’s University Incident Response Plan” (“TWU IRP”) which:

a. Addresses incident preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with Information System recovery and reconstitution planning activities;

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly; and

d. Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the university.

D. Incident Monitoring

TWU 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.

E. Incident Reporting

1. Users shall immediately report suspected or known security incidents to immediate supervisors and the Information Security team by reporting the suspicious activity to the Technology Service Desk via the Service Request System.

2. The ISO shall report Security Incidents to DIR for events that are assessed to:

    a. Propagate to other state systems;

    b. Result in criminal violations that shall be reported to law enforcement; or

    c. Involve the unauthorized disclosure or modification of Confidential Information, e.g., sensitive personal information as defined in §521.002(a)(2), Business and Commerce Code, and other applicable laws that may require public notification.

3. If the Security Incident is assessed to involve suspected criminal activity (e.g., violations of Chapter 33 or Chapter 33A Texas Penal Code), the security incident shall be investigated, reported, and documented in a manner that restores operation promptly while meeting the legal requirements for handling of evidence.

4. TWU Information Security shall submit summary reports of security-related events to DIR on a monthly basis.

F. Incident Response Assistance

1. TWU Information Security shall provide a Security Incident Response support resource that offers advice and assistance to Users of the Information System for the handling and reporting of security incidents. Users may request assistance using the Service Request System on the support resource.

G. Incident Response Plan

1. ITS maintains the TWU IRP that:

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

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

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

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

    e. Defines reportable incidents;

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

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

h. Addresses the sharing of incident information;

i. Explicitly designates responsibility for incident response to the ISO; and

j. Is protected from unauthorized disclosure and modification.

2. The TWU IRP is created, maintained and tested by TWU Information Security annually.

3. The TWU IRP is distributed to personnel with incident response roles and responsibilities.

4. The TWU IRP is reviewed and updated by the ISO annually.

5. Changes to the TWU IRP are communicated to appropriate ITS staff.

6. The TWU IRP is approved by the Chief Information Officer or Information Resource Manager annually.

H. Information Spillage Response

1. Information System Owners are responsible for responding to Information Spills by:

a. Identifying the specific information involved in the Information System contamination;

b. Alerting TWU Information Security by reporting the Information Spillage via the Service Request System or via a method of communication not associated with the spill;

c. Isolating the contaminated Information System or Information System component;

d. Eradicating the information from the contaminated Information System or Information System component;

e. Identifying other Information Systems or components of Information Systems that may have been subsequently contaminated; and

f. Perform any other additional actions deemed necessary during the incident response process.

II. Regulatory Compliance

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

1. IR-1, IR-2, IR-4, IR-5, IR-6, IR-7, IR-8, and IR-9.

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

Department of Information Resources Security Standards Catalog

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

Texas Business and Commerce Code § 512.053

Texas Government Code § 2054.518

Texas Government Code § 2054.1125

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

URP 06.200: Student Code of Conduct

TWU Security Incident Response

FORMS AND TOOLS

TWU Service Request System – Security Incident Response and Vulnerability Reporting

DIR SPECTRIM Reporting System

Publication Date: 07/02/2021

Revised: 02/02/2022; 01/08/2024