Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Information System Contingency Planning**
Regulation and Procedure Number:	**URP: 04.775**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

This University Regulation and Procedure ("URP") provides a mechanism for managing risks from information asset disruptions, failures, and disasters through the establishment of an effective contingency planning program. The contingency planning controls help Texas Woman's University ("TWU") implement security best practices regarding logical security, account management, and remote access.

APPLICABILITY

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

DEFINITIONS

1. "Contingency Plan" refers to interim measures to recover information technology services and resources after an emergency or system disruption.

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" means any individual not affiliated with TWU.

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, 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. "National Institute of Standards and Technology (NIST)" is a non-regulatory agency of the United States Department of Commerce that works in cooperation with various industries to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology.

6. "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.

7. "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. General Guidelines

A. This URP is applicable to all Information Resources owned or operated by TWU. All Users are responsible for adhering to these regulations and procedures.

B. The processes, procedures, controls, and standards established to meet the requirements of this URP shall incorporate: (1) TAC Title 1, Part 10, Chapter 202; (2) NIST Special Publication 800-53 (Rev. 5); (3) the Texas Security Control Standards Catalog, Version 1.3 (2/26/2016); and (4) other required information protection standards as applicable. The State of Texas

has chosen to adopt the contingency planning principles established in NIST SP 800-34 “Contingency Planning” guidelines. The NIST CP controls have been assigned a number; however, the State of Texas has not adopted every NIST CP control, so there are gaps in the numbering sequence. The following subsections outline the CP standards and TWU’s regulations and procedures.

II. CP-1 Contingency Planning

A. Regulation:

TWU must maintain a written Contingency Plan so that the effects of a disaster on Information Resources will be minimized, and TWU will be able to either to maintain or quickly resume mission-critical functions.

B. Procedure:

IT Solutions (“ITS”) shall develop, document, and disseminate a written set of controls that addresses the Contingency Plan for Information Resources. These controls should include the purpose, scope, roles, responsibilities, management commitment, coordination among TWU entities, and compliance.

III. CP-2 Contingency Plan

A. Regulation:

1. TWU must develop a Contingency Plan for the Information Resources that:

a. Identifies essential missions and business functions and associated contingency requirements;

b. Provides recovery objectives, restoration priorities, and metrics;

c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

e. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

f. Is review and approved by the Vice President for Finance and Administration.

2. TWU must securely communicate and distribute copies of the Contingency Plan to appropriate personnel. TWU must also coordinate contingency planning activities with incident handling activities.

B. Procedure:

1. ITS shall maintain a Contingency Plan for the Information Resources that includes:

a. Mission critical Information Resources, to include internal and external points of contact for personnel that provide or receive data or support interconnected systems and supporting infrastructure such as electric power, telecommunications connections, and environmental controls;

b. Disruption impacts and allowable outage times, to include effects of an outage to assess maximum allowable time access to an Information Resource may be interrupted before inhibiting performance of an essential function or to assess cascading effects on related or associated resources, systems, or processes;

c. Relevant recovery priorities, such as preventative controls, processes, techniques, or technologies for backup power, backup methodologies, environmental sensors and alarms, software and hardware replacement, and implementation roles and responsibilities;

d. Cost-benefit analysis to weigh the cost of implementing preventative measures against the risk of loss from not taking action;

e. Disaster recovery plan for major or catastrophic events that deny access to Information Resources for an extended period, contain measures addressing the impact or magnitude

of loss or harm resulting from an interruption, identify recovery resources, contain implementation instructions, and include provisions for annual testing;

2. ITS shall securely communicate and distribute copies of the Contingency Plan to appropriate personnel.

IV. CP-3 Contingency Training

A. Regulation:

TWU must provide periodic training for Employees in their contingency roles and responsibilities.

B. Procedure:

ITS shall develop and implementing procedures to train Employees in their roles and responsibilities relating to the Contingency Plan. Training must be provided upon assignment to a position that includes a role or responsibility relating to the Contingency Plan, or significant changes in the configuration of Information Resources.

V. CP-4 Contingency Plan Testing

A. Regulation:

TWU must test the Contingency Plan annually to determine the effectiveness of the plan, review the test results, and initiate corrective actions, if needed.

B. Procedure:

ITS shall test, reassess, and maintain the Contingency Plan annually. The test may be conducted virtually or through the simulation of an actual event. Tests shall be document and results used to initiate any necessary corrective actions. If an actual event occurs that requires that the Contingency Plan be executed, that event fulfills the annual test requirement.

VI. CP-6 Alternate Storage Site

A. Regulation:

TWU must establish an alternate storage site including necessary agreements to permit the storage and recovery of information asset backup information. TWU must ensure the alternate storage site provides information security safeguards equivalent to the primary site.

B. Procedure:

ITS shall maintain geographically independent server rooms where data is stored in a secure, environmentally safe, locked facility accessible only to TWU representatives. Primary information systems located in Denton and Dallas are backed up daily and these daily backups shall be copied to an offsite backup location for disaster recovery purposes.

VII. CP-9 Information System Backup

A. Regulation:

TWU must conduct backups of Information Resources within defined recovery time and recovery point objectives. TWU must conduct backups of User-level and system-level information contained in the information system, and documentation including security-related documentation. TWU must protect the confidentiality, integrity, and availability of backup information at storage locations.

B. Procedure:

ITS shall establish a process that provides for daily, weekly, and monthly backups, scheduled on a per information system basis. The frequency of the backup depends on the application requirements and nature of data stored.

VIII. CP-10 Information System Recovery and Reconstitution

A. Regulation:

TWU must provide for the recovery and reconstitution of Information Resources to a known state after a disruption, compromise, or failure.

B. Procedure:

ITS shall ensure that Information Resources defined as critical in the Contingency Plan are backed up daily to a geographically separate data center. ITS ensures that Information Resources not defined as critical in the

Contingency Plan are recoverable depending on application requirements and nature of data stored.

IX. 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

1 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