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 and Information Technology Solutions**

POLICY STATEMENT

This University Regulation and Procedure ("URP") provides a mechanism for managing risks from Information Resource disruptions, failures, and disasters through the establishment of an effective contingency planning program. The contingency planning controls help Texas Woman's University ("TWU") to minimize the effects of a disaster on Information Resources, and maintain or quickly resume mission-critical functions.

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 Students, Employees, University Affiliates, 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, 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” is a discrete set of Information Resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

6. “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.

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, or 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 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. Contingency Plan

1. Institution-wide emergency plans are maintained by TWU Risk Management, per URP 04.410: Emergency Management and Business Continuity. Risk Management maintains the Texas Woman's University Continuity of Operations Plan ("COOP").

2. The Chief Information Officer ("CIO") is responsible for developing a Contingency Plan for Information Resources that:

a. Identifies mission-critical Information Resources and business functions and associated contingency requirements;

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

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

d. Addresses maintaining essential mission and business functions despite a disruption, compromise, or failure;

e. Addresses eventual, full Information System restoration without deterioration of the controls originally planned and implemented;

f. Addresses the sharing of contingency information; and

g. Is reviewed and approved by the CIO.

3. The CIO shall:

a. Securely communicate and distribute copies of the Contingency Plan to appropriate personnel;

b. Coordinate contingency planning activities with incident handling activities;

c. Review the Contingency Plan for the Information System annually;

d. Update the Contingency Plan to address changes in the organization, Information System, or environment of operation and problems encountered during plan implementation, execution, or testing;

e. Communicate Contingency Plan changes to the appropriate personnel;

f. Incorporate lessons learned from Contingency Plan testing, training, or actual contingency activities into the Contingency Plan; and

g. Protect the Contingency Plan from unauthorized disclosure and modification.

B. Contingency Training

1. The CIO, or their designee, shall develop and implement 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. Training will be provided upon changes to the Contingency Plan and periodically thereafter.

2. Contingency training content shall be reviewed and updated periodically and following changes to the organization, Information System, or environment of operation.

C. Contingency Plan Testing

1. The CIO, or their designee, 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 documented 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.

D. Alternate Storage Site

1. IT Solutions ("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. The alternate storage site shall provide controls equivalent to those of the primary site.

E. Telecommunications Services

1. ITS shall establish alternate telecommunications services, including necessary agreements to permit the resumption of mission critical operations for essential mission and business functions within a reasonable time period as defined within the TWU Continuity of Operations Plan when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

F. Information System Backup

1. ITS or a University Affiliate shall conduct backups of Information System-level information (including Information System state information), critical user-level information contained in the Information System, and Information System documentation, including security- and privacy-related documentation.

2. The confidentiality, integrity, and availability of backup information shall be protected by security control mechanisms based on risk decisions.

3. ITS provides for daily, weekly, and monthly backups, scheduled on a per Information System basis. The backup and frequency depends on the application requirements and nature of data stored.

G. Information System Recovery and Reconstitution

1. 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. The recovery and reconstitution of an Information System to a known state shall be provided within the specified recovery time and recovery point objectives defined in the Contingency Plan.

2. ITS shall ensure that Information Resources defined as critical in the Contingency Plan are resilient. This may include load-balancing, off-site replication, and service monitoring.

H. Alternate Communications Protocols

1. ITS shall provide the capability to employ alternative communications protocols in support of maintaining continuity of operations based on risk management decisions.

II. Regulatory Compliance

A. The State of Texas has chosen to adopt a select number of Contingency Planning (“CP”) principles established in NIST SP 800-53 “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 included in TWU’s regulations and procedures.

1. CP-1, CP-2, CP-3, CP-4, CP-6, CP-8, CP-9, CP-10, and CP-11.

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

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

Texas Labor Code § 412.054

URP 01.320: University Policy Development and Implementation

URP 04.410: Emergency Management and Business Continuity

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

FORMS AND TOOLS

None

Publication Date: 07/02/2021

Revised: 12/15/2021; 08/05/2024