ITS Business Continuity Management System Policy

Version: 4 Effective
Date: January 30, 2024

Policy Summary:

This policy defines a business continuity management system (BCMS) that outlines business continuity and disaster recovery plans, processes, procedures, testing, and reporting mechanisms that are to be in effect to provide continuity of Information Technology and Security (ITS) operations in the event of a disaster. This provides the structure for building operational resilience and capability for an effective response that safeguards university data and assets of its key stakeholders during a disruption. Information Technology and Security (ITS) is required to have controls in place that provide reasonable assurance that security and operational objectives are addressed throughout a disruption for key campus services. This does not define recovery procedures for SaaS, Cloud, or hosted applications the university may utilize to deliver business functions.

Questions regarding this policy should be directed to utcio@ut.edu.

Applicability/Eligibility:	Exceptions:
This policy applies to Information Technology and Security. The scope of the Business Continuity Management System may be amended based on the needs of the University.	None

Policy Administration:

Mandating Authority:
(Check all that apply)

- Federal Law
- University President
- Other: (specify)
- State Law or Regulation
- Accrediting Body

Responsible Office/Dept/Committee(s):

Name	Campus Address

Name	Title	Phone Number
Tammy Loper	Vice President, Information Technology and Security	813-257-7522

Policy Management:

Policy History:

Date	Version	

responsibilities

d. Primary and Alternate Contact Lists

6. Damage Assessment
7. Recovery Plans
    a. Critical System Recovery
        i. Prioritization of recovery
        ii. Interdependencies
        iii. Resource requirements
        iv. Security controls
        v. Continuation of operations
            1. Mobilizing alternate locations / resources
            2. Managing alternate locations / resources
            3. Critical system support
                a. Short term
                b. Long term

5. ITS will securely store copies of plans and supporting materials in a remote location; at a sufficient distance to escape any damage from a disaster at the university's main campus and be available via remote connection (Office 365 etc.).

6. ITS will have appropriate mechanisms to ensure that plans remain current and updated between annual tests and reviews accounting for:
    1. Change management implications
    2. New/Major upgrades of system implementations
    3. New policy adoption
    4. New contract implementations
    5. New threat/risk identification
    6. Staff/resource/responsibility changes

7. ITS will publish plans and sufficiently train any and all individuals that are required or responsible for supporting the BCP.

Definitions:

Business Continuity: Capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident
[SOURCE: ISO 22301Td [(22)10 (301Td [(22)10 (301Td [(22)P (l)6 (o)10 (w)6 (i)6 (ng a)10 (pw -8.98 -1

Additional Information and Resources:

Reference:

ISO/IEC 22301:2019(E) Societal security – Business continuity management systems – Requirements. Geneva, Switzerland: ISO/IEC.