ITS Business Continuity Management System Policy

Version: 3.1
Effective Date: 12/12/2017

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 the Managing Director, IT Operations at 813-257-3277.

Applicability/Eligibility:
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.

Exceptions:
None

Policy Administration:

Mandating Authority: (Check all that apply)

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

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology and Security, Managing Director of IT Operations	East Walker Hall 121	813-257-3277

Responsible Executive(s):

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

Policy Management:

Policy History:

Date	Version	Reason for Change
12/14/2015	1.0	Initial policy draft
12/21/2015	1.0a	Pre-Approval revision
3/10/2016	2.0	Incorporating Organizational Changes
11/29/2017	3.0	Incorporating Organizational Changes, Updated the Policy Summary, Added Policy Statements
12/10/2019	3.1	Updated to ensure consistency with other ISO management system polices.

Policy Approvals and Reviews:

Date	Organizational Group
3/12/2021	President
3/12/2021	Senior Staff

Web Links:

Policy Link: https://www.ut.edu/bcms

Full Policy Text:

Business Continuity Management System requirements:

Leadership. Senior Staff and all levels of management covered by the scope of this policy are committed to the Business Continuity Management System (BCMS) and support all activities related to this endeavor.

Planning. Information Technology & Security (ITS) will develop a plan to review and test the BCMS annually.

Operational Procedures. ITS will develop processes and procedures related to business continuity within the scope of this policy. An ITS Business Continuity Plan will be developed as part of this exercise.

Performance Assessment. Annual tests will be performed to determine current applicability of processes and procedures as part of the BCMS. Tests will be planned and documented for review and, where applicable, areas of improvement cited.

Improvement Plans. ITS will develop improvement plans based on the results of performance assessments conducted. Improvement plans will be documented and reviewed for completeness.

Risk Management. ITS will complete risk assessments using ISO/IEC 27005:2011 - Information Security Risk Management and the National Institute of Standards and Technology's Special Publication 800-53, Security and Privacy Controls for Federal Systems and Organizations.

Internal Audit. Internal audits of the business continuity management system shall be conducted annually. Personnel who are independent of the current work or project shall be retained to perform internal audits.

Management Reviews. Management reviews will be conducted by ITS at various intervals.

Non-conformity and corrective actions. Business continuity management system nonconformities and corrections will be documented and maintained by ITS.

ITS departments notified about corrective actions must submit a corrective action plan to the BCMS manager within 30 days. A notable exception is that corrective actions resulting from British Standards Institution (BSI) certification audits must be submitted within 15 days, to provide time for the BSI auditor to accept the corrective action plan(s).

Records Retention. Unless specified otherwise, business continuity management system records will be maintained electronically by ITS for a minimum of three (3) years.

Training. All ITS departments included in the business continuity management system scope shall be made aware of the relevance and importance of their information security activities and how they contribute to the achievement of goals and objectives. ITS will provide training for business continuity management system participants.

Policy Statements:

1. ITS will develop, implement, test and maintain a Business Continuity Plan (BCP) for all Information Technology and Security resources that deliver or support university systems and services.

2. ITS will conduct risk assessments to identify, estimate, and prioritize risks to university operations and conduct business impact analyses to identify all critical functions of their supporting information systems.

3. ITS will define and document the details necessary to effectively respond, manage, and recover from either a service disruption incident or a catastrophic event.

4. ITS, at a minimum, is to include the following documentation and procedures in their business continuity plan and its supporting components:

1. Scope / Objectives
2. Risk Evaluation and Required Security Controls
3. Business Impact Analysis
4. Communications Procedures
5. Business Continuity Plan Organization Structure
    a. Activation of plans
    b. Succession of Authority Procedures
    c. Business continuity emergency incident response team roles and 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 22300]

Business Continuity Management System (BCMS): Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity.
[SOURCE: ISO 22301]

Business Continuity Plan: Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following a disruption.
[SOURCE: ISO 22301]

Additional Information and Resources:

Reference:

ISO/IEC 22301:2012(E) Societal security – Business continuity management systems – Requirements. Geneva, Switzerland: ISO/IEC.