THE UNIVERSITY OF TAMPA
INFORMATION TECHNOLOGY AND SECURITY

# ITS Business Continuity Management System Policy

Version: 4.1
Effective Date: November 11, 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:**
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 / AVP IT Operations | Jenkins Technology Building 381D | 813-257-5372 |

Responsible Executive(s):

| Name | Title | Phone Number |
| --- | --- | --- |
| Tammy | | |

**Additional Information and Resources:**

**Reference:**

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