THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0311-HSC-B Business Continuity Planning	
Version 3	**Effective Date: 03/13/2018**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish requirements for the development of formal documented contingency plans for the University of Tennessee Health Science Center (UTHSC) IT Resources to maintain and resume normal business operation, recovering from an emergency, disaster, or other extraordinary disruption. The overall goal is to ensure that all departments and business units of the University are prepared to rapidly restore critical functions in the aftermath of any emergency or disaster.

Scope

All UTHSC IT Resources deemed necessary (critical system) to recover essential business functions or dependent business functions.

Definitions

Business Impact Analysis (BIA): An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Critical functions: functions required to enable, support, and implement the safekeeping of our students, staff, and visitors and facilitate the resumption of academic, research, and administrative programs.

Critical systems: a UTHSC IT Resource having attributes including, but not limited to:

a. Any system containing the authoritative copy of UTHSC data or information with a level 2 categorization using the guidelines outlined in IT0005-HSC-A-Data & System Categorization.
b. Any system requiring contingency plans as prescribed by Federal or State statutes or regulations.
c. Any system identified as having a Recovery Time Objective (RTO) or less than 24 hours.
d. Deemed critical by the Business Impact Analysis (BIA).

Data owner: The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division.

Disaster: Any IT incident that is determined to have potential impacts on the business continuity and ongoing operations of UTHSC.

- **Major Disaster:** A major disaster will normally have extensive damage to system hardware, software, networks, and/or operating environment.
- **Minor Disaster:** A minor disaster will be characterized by an expected downtime of well below the RTO determined in the business impact analysis, and minor damage to hardware, software, and/or operating environment.

Recovery Time Objective (RTO): The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.

System owner: Person or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system

UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.

Responsibilities

Office of Cybersecurity is responsible to:

- Develop a contingency plan template that guides data and system custodians and owners through all required elements.
- Ensure all contingency planning requirements and activities comply with UTHSC policies; local, state, and federal laws and guidelines.
- Advise the Data or System Custodian and the Data or System Owner about the technical aspects of these duties.

Data and System Custodian in close collaboration with the Data and System Owner is responsible to:

- Develop the contingency plan containing all required elements for the UTHSC IT Resource within scope.
- Implement processes and procedures meeting all requirements and activities outlined in the Contingency Plan.
- Establish documented procedures necessary to back-up and restore any data as well as for providing coverage for the systems under their responsibility that is consistent with good business resumption planning.

- Establish documented procedures detailing periodic testing to ensure data can be retrieved and restored from the backups and normal business operations can be resumed.
- Train those who have responsibilities in the plan.

Data and System Owner is responsible for approving the plan and reviewing the plan on the timeline provided below.

Standard

Business Continuity / Disaster Recovery Plan

1. For all UTHSC IT Resources within scope, a contingency plan must be developed that addresses business continuity, emergency mode operation, and recovery from an emergency, disaster, or other extraordinary disruption.
2. Requirements of the contingency plan should include, but not limited to:
    - Activation Authority
    - Points of Contact
    - Emergency Points of Contact Outside of the Unit
    - Identification of Information Assets and Risk Assessment
    - Identification of Crucial Assets and Dependencies: Development of Contingency Plans
    - Preparation Checklists
    - Data backup procedures and offsite storage locations
    - Data restoration procedures
    - Records of Testing procedures for restoration from backup
    - Records of Training
    - Records of Testing Contingency Plan
    - Mission Crucial System History
3. Each IT Resource within scope will have a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) identified based on the business impact analysis (BIA).
4. The RTO is determined based on the following categories:
    a. Business Impact Nominal – Data is unavailable for over 2 weeks with minimal to no impact on organizational operations, organizational Assets, or individuals.

b. Business Impact Low – Data is unavailable for 72 hours to 2 weeks, and it could be expected to have an adverse effect on organizational operations, organizational Assets, or individuals.
c. Business Impact High – Data is unavailable for 72 hours or less and it could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational Assets, or individuals.
d. Business Impact Critical – Data is related to control Systems that support the University, but if subverted, could be life-threatening to University Employees, students, and others using University facilities (e.g., attending athletic events).

5. A documented record will be maintained for all UTHSC IT Resources designated as critical (within scope). The record will document system outages, downtimes, failures, data loss, and major maintenance. This record shall be available for inspection by the UTHSC Office of Cybersecurity.

Review

1. This plan is reviewed and updated, at a minimum:
   a. Annually
   b. In response to environmental or operational changes that affect any part of the plan.
   c. Following any exercise of any portion of the plan, which reveals deficiencies.

Documentation

1. Offsite copies of the latest revision of this plan are maintained by:
   a. System Owner
   b. System Custodian
   c. Other key personnel responsible for the execution of the plan.
2. The System Owner reviews and approves the plan annually. The System Owner signs and dates the plan signifying such approval and keeps a copy of the most current version of the plan both onsite and offsite.
3. The Data Custodian forwards a copy of the most recent version of the approved plan to the UTHSC Office of Cybersecurity annually.
4. The System Owner approves reviews and changes to the plan made between annual reviews. A record of changes and reviews shall be maintained at the front of the document.

Training

1. The System Custodian is responsible for conducting training annually and at each change in the plan for those who have responsibilities under the plan. Training on changes need only be provided to personnel directly affected.
2. Recovery teams and users shall be trained to understand and know their role in the business recovery process.
3. The System Custodian shall maintain a record of training and who attended, and a summary of the content of the training.

Testing

1. The plan is tested on an annual basis. A written document of test findings is made by the System Custodian and approved by the System Owner.
2. The System Owner may approve exceptions to exercise contingency plans.
3. It is permissible to exercise various elements of the plan in phases, or at different times during the year. This is not an exception to the requirement to exercise the plan.

Reporting

1. Completion of annual training and exercise of the plan, and documentation of any exceptions, shall be forwarded to the Office of Cybersecurity annually.
2. Report of annual completion of contingency plan review shall be forwarded to the Office of Cybersecurity.
3. The Office of Cybersecurity or designee is to provide within 30 days of the annual reporting deadline, to the Office of the CIO, a summary report of:
   a. Those Contingency Plans that have not completed annual training or have failed to report its completion.
   b. All approved exceptions to exercise contingency plans.
   c. Those contingency plans that have not been tested or failing to report on testing of the contingency plan.
   d. Status of contingency plans review and updates.
4. The Office of the CIO shall initial the summary report and be responsible for retention.

IT Resource Backups

Disaster recovery is an integral part of the overall business continuity plan that ensures that technology that supports the business of the university will continue

after an event occurs. Backups of data and systems which contain information necessary to maintain and resume normal UTHSC business functions is required. These backups would be used in case of an emergency or other occurrence that results in the loss, destruction, theft or corruption of such information and systems

1. A retrievable exact copy (Backup) of all UTHSC data within scope is to be maintained on a documented schedule determined to be appropriate by the Data Custodian in conjunction with the Data Owner, or his/her delegate. This determination shall be based on the characteristics and criticality of the data. This backup requirement extends to essential or authoritative data stored on personal computers as well as shared systems.
2. A Backup of all UTHSC data or information with a classification rating of 3 in any area must be obtained before moving any equipment.
3. Backup copies of applications and data associated with IT Resources within scope shall satisfy emergency planning and requirements for disaster recovery as well as business continuity operations of any application or system dependent upon such data.
4. On a periodic basis, or as needed in response to environmental and/or operational changes the documented backup procedures must be reviewed and updated.
5. Backups must be moved to a secure off-campus location in a secure and timely manner per documented procedures.
6. Backup media must have at a minimum the following identifying criteria:
   a. IT Resource name
   b. Creation Date
   c. HSC Contact Information
7. Backups of essential data for disaster recovery purposes shall be stored at a secure, off-campus site that provides a level of protection commensurate with the criticality of the data.
8. Backups of UTHSC data or information with a classification rating of 3 in any area must be encrypted if the physical security of the stored backup copies is at risk.
9. Backup and other retention services for data must comply with University of Tennessee data retention policies as specified in UTSA-FI0120-Records Management.
10. Disposition schedules that destroy electronic information resources must be suspended if those resources are subject to a litigation hold.

UT Health Science Center: IT0311-HSC-B Business Continuity Planning	
Version 3	**Effective Date: 03/13/2018**

Policy History

Version #	Effective Date
1	03/13/2018
2	05/12/2022
3	03/01/2025 – new naming convention

References

1. IT0311-Information Technology Data Access Management and Recovery
2. UTSA-FI0120-Records Management
3. IT0005-HSC-A-Data & System Categorization
4. NIST Glossary of Terms