THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0311-HSC-C Information Security during a Disaster	
Version 5	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 specify required treatment of Information Resources and systems in the case of an emergency or other events resulting in the loss, destruction, theft, or corruption of the University of Tennessee Health Science Center (UTHSC) IT Resources, an inability to access information that cannot be resolved in a reasonable time period, or damages to systems which are necessary for the maintenance of confidentiality, integrity and availability of information.

Scope

All UTHSC IT Resources and systems.

Definitions

Disaster – a sudden event, such as an accident or a natural catastrophe, that causes great damage or loss of life.

Level 2 Data - The effect on confidentiality and integrity of the Data is significant and includes compliance requirements. This Data is governed by federal, or state compliance requirements, and unwarranted exposure can lead to compliance issues and/or fines. This includes all Data that contains personally identifiable information (PII), protected health information, student education records, and cardholder Data. This categorization level also includes lower-risk items that, when combined, represent increased risk. per IT0005-HSC-A-Data & System Categorization. Minimum security requirements are explained on the webpage https://uthsc.edu/its/cybersecurity/requirements.php.

System Security Plan (SSP) – formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

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

System owners are responsible for the development of the documentation of a Business Continuity/Disaster Recovery Plan in which this is a part.

Standard

1. In the case of disaster:
   a. During all phases of a disaster (including, but not limited to, preparation for an impending event, the immediate aftermath of the event, implementation of contingency plans, subsequent recovery and return to normal operation) all policies, laws and regulations required to be followed governing the UTHSC Information Security Program shall remain in effect.
   b. Documented procedures to enable the continuation of critical business processes for the protection of the security of all UTHSC data or information shall be maintained. For systems with a Level 2 data categorization (per IT0005-HSC-A-Data & System Categorization), this should be part of their System Security Plan (SSP). In support of this requirement:
      i. Copies of written procedures shall be retained offsite or electronic copies that can be accessed remotely will be retained.
      ii. Software and systems that are necessary for the continuation of these business processes shall be documented as ~~a~~ part of these procedures. The procedures shall specify how, and in what time frame after their loss or compromise the functionality of these processes shall be restored.
2. Theft of data during a disaster shall be treated as an information security incident and will be handled according to IT0017-HSC-A-Security Incident Response. If data have been stolen, there has been unauthorized access to, or use of, these data, the integrity and validity of these data shall be verified prior to further use.

Policy History

Version #	Effective Date
1	03/13/2018
2	03/26/2020
3	05/12/2022
4	01/11/2023
5	03/01/2025 – new naming convention

References

1. UTHSC Information Security Program
2. IT0311-Information Technology Data Access, Management, and Recovery
3. IT0005-HSC-A-Data & System Categorization
4. IT0017-HSC-A-Security Incident Response