THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: CP-002-Infomation Security during a Disaster	
Version 3	Effective Date: 03/13/2018

Responsible Office: Office of Cybersecurity	Last Review: 3/26/2020 Next Review: 3/26/2022
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 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. These events shall be referred to collectively and severally as "disaster."

Scope

All UTHSC IT Resources and systems.

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 continuation of critical business processes for the protection of the security of all data or information with a classification rating of 3 in any area shall be maintained. 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 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 Standard-InfoSec-IR-001-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.

References

1. GP-002-Data & System Classification
2. UTHSC Information Security Program
3. IR-001-Security Incident Response.