THE UNIVERSITY OF TENNESSEE CHATTANOOGA

UTC-S-IT0128 – UTC Contingency Planning Standard

Objective:
To align University of Tennessee at Chattanooga (UTC) standards of practice with University of Tennessee System-wide policy for developing, maintaining and documenting a Contingency Planning program.

Scope:
This program applies but is not limited to employees, contractors, agents, and representatives accessing, using, or handling UTC information technology resources.

Principles:
This document is a UTC-specific Standard based on University System-wide policy. Each User of UTC resources is required to be familiar and comply with University policies, and acceptance is assumed if the User accesses, uses, or handles UTC information technology resources.

The Chief Information Officer (CIO) is the Position of Authority (POA) for Information Technology at UTC and responsible for IT security at the University of Tennessee Chattanooga.

Responsibilities:

1. The CIO has overall responsibility of the Contingency Planning (CP) program at UTC and ensures:
    a. The program is developed, documented, and disseminated to appropriate UTC entities in accordance with University policy.
    b. The program is reviewed and updated annually.
    c. An alternate data storage location is established in the event that the primary storage location is not available.
    d. An alternate processing site is established that permits the transfer and resumption of mission-essential functions when primary processing capabilities are unavailable.

    NOTE: The CIO determines what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are concerning for UTC.
2. The Chief Information Security Officer (CISO) is responsible for overseeing the Contingency Planning program and consulting system owners to ensure effective procedures are implemented.
3. System owners/administrators are responsible for developing appropriate department-level procedures for their respective system(s).

Standard:

1. All business systems supporting mission-essential functions are included in UTC's Contingency Planning program.
2. The CISO will ensure:
    a. Documentation exists for an alternate storage site and its requirements.
    b. Documentation exists for an alternate processing site and its requirements.

c. User-level and system-level backups are consistent with system recovery time and recovery point objectives.
d. Some facet of the IT system is tested in a Disaster Recovery scenario annually and sufficiently documented.

3. System owners will:
    a. Develop, document, and maintain a contingency plan for their information system that:
        i. Identifies essential missions and business functions that must continue and/or be restored in the event of a outage.
        ii. Provides recovery objectives and restoration priorities.
        iii. Addresses roles, responsibilities, and assigned individuals with contact information.
    b. Provide documented staff contingency training.
    c. Test backup information periodically to verify media reliability.

References:

UT Policy IT0128 – Contingency Planning