THE UNIVERSITY OF TENNESSEE
CHATTANOOGA

UT - Chattanooga:	
IT0129-C - UTC Standard: Physical and Environmental Protection	
Version: 1	Effective Date: 08/10/2018

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 Physical & Environment Protection 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 Physical & Environmental Protection (PE) 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.
2. The Chief Information Security Officer (CISO) is responsible for overseeing the Physical & Environmental Protection program and consulting system owners to ensure effective procedures are implemented.
3. System owners/administrators are responsible for developing department-level procedures for their respective system(s).

Standard:
1. All business systems supporting mission-essential functions are included in UTC's Physical & Environmental Protection program.
2. System owners will:
    a. Develop, document, and maintain a list of individuals with authorized access to facilities housing business-critical information systems.
    b. Verify individual access authorizations before granting access to the facility.

    c. Maintain physical access audit logs for visitors to the facility. **NOTE:** *Individuals with permanent physical access authorization credentials are not considered visitors.*

    d. Provide visitors with escort and monitor visitor activity when individuals have access to systems classified as HIGH and there is potential for severe impact to the University should there be a security breach.

3. Properly secure physical access devices and update records when access devices are lost, compromised or individuals are transferred or terminated.
4. Ensure an appropriate level of controlled access to information system output devices.
5. Ensure enough short term uninterruptible power is available to critical system components in the event of a primary power outage.

References:

[IT0129 - Physical and Environmental Protection](#)