THE UNIVERSITY OF TENNESSEE CHATTANOOGA

UTC Media Protection 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 Media 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 Media Protection (MP) 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 Media Protection program and consulting system owners to ensure effective procedures are implemented.
3. System owners/administrators are responsible for adhering to this Standard for their respective system(s).

Standard:

1. All business systems supporting mission-essential functions are included in UTC's Media Protection program.
2. System owners and administrators must develop, document and maintain Media Protection processes and procedures that address:
    a. Restricting access to digital and non-digital information media that contains sensitive data.
    b. Control of all digital and non-digital sensitive information within access-controlled, secured storage areas.
    c. Protecting information media until the media are destroyed or sanitized.
    d. Accountability of authorized personnel and protection of sensitive information and/or media during transport outside of controlled areas.

    e. Obtaining and submitting the UTC Business Services' Warehousing Services' *Computer/Hard Drive Surplus Form & Certification of Sanitization* form for hard disk erasure.
3. UTC Warehousing Services must develop, document and maintain procedures that:
    a. Provides media sanitization for computer hard drives and other electronic storage devices.
    b. Ensures all media installed within surplus devices (i.e. hard drives still installed in the computer) is erased per fiscal policy to DoD standards. This includes copiers with hard drives.
    c. Ensures, if a hard disk cannot be wiped for any reason, that it is shredded, and UTC receives a certificate of destruction.
4. Note: Please refer to the *Guidelines for Handling Paper-based University Data* available on the UTC IT Security website, https://www.utc.edu/information-technology/security/policies-guides-plans.php

References: