UT - Chattanooga:	
IT0125-C - UTC Standard: Configuration Management	
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 Configuration Management program.

Scope:
This program applies to all UTC employees and affiliates responsible for performing system administration duties for 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 Configuration Management (CM) 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 Configuration Management 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 Configuration Management program.
2. All system owners/administrators must ensure Configuration Management procedures:
    a. Address roles, responsibilities, and configuration management processes.
    b. Establish a process for identifying and managing system configurations, configuration retention and annual reviews and updates of the procedure(s).

c. Provide for a Baseline Configuration.
d. Establish Configuration Change Control including:
    i.   Types of changes subject to a change control process for the information system.
    ii. Review and approval process for proposed changes.
    iii. Change decision records and retention.
    iv. Implementation of approved changes to the information system.
    v.   Configuring systems to provide only essential capabilities and restricting use of non-essential services, functions, ports, protocols, etc.

References:

IT0125 - Configuration Management