UT - Chattanooga: IT0131-C - UTC Standard: Security Assessment and Authorization	
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 Security Assessment & Authorization 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 Security Assessment & Authorization (SA) 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.
1. The Chief Information Security Officer (CISO) is responsible for overseeing the implementation of the Security Assessment & Authorization program and consulting system owners to ensure effective procedures are implemented.
2. 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 Security Assessment & Authorization Protection program.
2. The CISO will ensure:
    a. The implementation of a continuous monitoring program for infrastructure and critical systems.

b. Development of a Plan of Action and Milestones (POAM) to correct system deficiencies, ensuring remedial actions are taken, and maintaining updates to POAM.

3. System owners/administrators will ensure procedures address:
    a. Plan scope, schedule of assessments and reporting.
    b. Verification of system boundaries and interconnections.
    c. Criteria and metrics for system monitoring and reporting of system status.

References:

IT0131 - Security Assessment and Authorization