THE UNIVERSITY OF TENNESSEE
CHATTANOOGA

UT - Chattanooga:
IT0134-C - UTC Standard: System & Communications 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 System & Communications 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 System & Communications (SC) 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 System & Communications 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 System & Communications Protection program.
2. System owners and administrators must develop, document and maintain procedures that address:
    a. Monitoring and mitigating the risk of Denial of Service attacks on networked systems.

b. Establishing critical system boundaries to protect against the unauthorized release of information or unauthorized communication through the boundary protection mechanisms

c. Ensuring critical systems are configured to deny network traffic by default and allow approved network traffic (i.e. deny all, permit by exception).

d. Ensuring all cryptographic keys are appropriately protected.

e. Prohibiting the remote activation of collaborative computing mechanisms (e.g. cameras, microphones, conferencing software, etc.).

f. Ensuring Address/Name resolution services are fault-tolerant and return appropriate, authoritative data in response to queries (e.g. digital signatures).

References:

IT0134 - System and Communication Protection