THE UNIVERSITY OF TENNESSEE
CHATTANOOGA

UT - Chattanooga: IT0120-C - UTC Standard: Secure Network Infrastructure	
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 Secure Network 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 IT0120. 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 Secure Network program at UTC.
2. The Chief Information Security Officer (CISO) is responsible for overseeing the Secure Network program.
3. The Technical Director has responsibility for disseminating network status to appropriate management and ensuring:
    a. The installation, connectivity to, and the maintenance of the network infrastructure.
    b. Monitoring and maintenance of UTC's network.
4. Network managers are responsible for adhering to this Standard for their respective system(s).

Standard:

1. UTC adopts and adheres to the University of Tennessee System-wide Policy for Secure Networks.
2. Network managers must develop and maintain procedures that ensures:
    a. Approved personnel access the infrastructure.
    b. Communications equipment is housed in dedicated enclosures and physical/logical controls are enforced 24x7x365.

c. Security controls are in place and networks appropriately isolated (VLAN) to protect compliance-regulated information and systems (e.g. FERPA, PCI, HIPAA, and PII.

d. A technology refresh cycle program is developed for maintaining the hardware and software currency of infrastructure components and avoiding end-of-life timeframes and lack vendor support.

e. Monitoring the infrastructure and maintaining network availability and integrity.

f. A network event logging and management strategy. The Network Architect must identify and document critical network components and ensure significant events are logged.

g. A sparing strategy for critical component.

h. Administrative access to network components utilizes secure access methods (e.g. ssh, https), or compensating controls are in place and documented when insecure protocols must be used.

References:
IT0120 - Secure Network Infrastructure