THE UNIVERSITY OF TENNESSEE CHATTANOOGA

UTC ACCESS CONTROL 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 an information and systems Access Control 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 Access Control program at UTC.
2. The Chief Information Security Officer (CISO) is responsible for overseeing the Access Control program.
3. System owners/administrators are responsible for ensuring users of their respective system(s) read and understand the following Standard.

Standard:

1. UTC adopts and adheres to the University of Tennessee System-wide Policy for Access Control to critical information and systems.
2. System managers must ensure appropriate procedures are established for:
    a. Creating, activating, modifying, and maintaining critical information system accounts.
    b. Controlling access to critical information systems by:
        i. Limiting access to authorized users, processes acting on behalf of authorized users, and devices.
        ii. Employing the principle of least privilege that limits access to only the types of transactions and functions that authorized users are permitted to execute.
        iii. Limiting consecutive unsuccessful login attempts and delaying the next login prompt.
        iv. Displaying an appropriate system use notification message that addresses use of UTC resources, privacy and acceptance of policy.
        v. Using session-timeouts and locking with pattern-hiding displays.

c. Automatic termination of user sessions.
d. Separation of duties to reduce the risk of collusion.
e. Ensuring non-privileged accounts access only non-privileged or security functions.
f. Managing all methods of remote access, employing encrypted sessions and ensuring appropriate protection to critical information and systems.
g. Establishing appropriate usage and implementation guidelines for wireless technologies.