UTC-S-IT0128 – UTC Audit and Accountability 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 Audit & Accountability 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 Audit & Accountability (AU) 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 Audit and Accountability 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 Audit & Accountability program.
2. All system owners/administrators must:
    a. Determine and document which events are deemed significant and relevant to the security of the system and audit logs should be maintained. (e.g. system, application, network, and user activity.)
    b. Ensure audit management procedures address:
        i. Type of event, when it occurred, where it happened, source of the event, outcome and associated system and/or individual(s).
        ii. Record protection and retention of system, application, security and event logs for a minimum of six months.
        iii. Event alerting and response.
        iv. Regular audit log review, analysis, and reporting.

References:
UT Policy IT0127 – Audit and Accountability