THE UNIVERSITY OF TENNESSEE CHATTANOOGA

UTC-S-IT0124 – UTC Risk Assessment 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 a Risk Assessment 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 Risk Assessment (RA) 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 Risk Assessment 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 Risk Assessment program.
2. The CISO will ensure:
    a. An IT Security Plan is submitted to the CIO annually and will include a status report in the following Cyber Security Framework functional areas:
        i. IDENTIFY – Asset Management, Business Environment, Governance, Risk Assessment, Risk Management.
        ii. PROTECT – Access Control, Awareness Training, Data Security (C-I-A), Information Protection & Procedures, Maintenance, Protective Technology.
        iii. DETECT – Anomalies, Continuous Monitoring, Detection Processes.
        iv. RESPOND – Planning, Communications, Analysis, Mitigation and Improvements.
        v. RECOVER – Planning, Improvements and Communications.
        vi. Other conditions that may impact the security posture of UTC.

b. A Tabletop Risk Assessment is performed annually
c. Continued mitigation of exposed sensitive information (SSN, Credit Cards, PII, etc.) on network shares and department computers.
d. Appropriate/approved industry standard vulnerability scanning tools and techniques for enumerating flaws and improper configurations must be employed.

3. The IT Security Team must perform:
    a. Continuous Systems & Network Monitoring to:
        i. Ensure perimeter protection by blocking public access to internal UTC resources.
        ii. Ensure internal core firewalling and LAN segmentation to protect business networks.
        iii. Utilize network IDS systems to monitor and log internal threats.
        iv. Ensure server and endpoint (client) protection. *(NOTE: Patch management is addressed in separate Systems & Information Integrity Standard.)*
    b. Monthly Vulnerability Scans of compliance-regulated business systems that require more frequent vulnerability scans to comply with federal, state or institutional regulations.
    c. Annual Vulnerability Scans non-compliance-regulated systems.
    d. A review of all Vulnerability Assessment reports, analysis and recommendations, and disseminate a plan of action to address any vulnerability.

References:
UT Policy IT0124 – Risk Assessment