UT - Chattanooga: IT0130-C - UTC Standard: Personnel Security	
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 Personnel Security 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 Personnel Security(PS) 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 Personnel Security program and consulting system owners to ensure effective procedures are implemented.
3. System owners/Managers are responsible for ensuring their staff reads and understands the following Standard.

Standard:

1. All critical business systems having mission-essential functions are included in UTC's Personnel Security program.
2. Managers must:
    a. **For Onboarding**: Ensure appropriate background checks are performed by HR before hiring and access is granted to any system categorized as Moderate or High impact.
    b. **For Terminations or Transfers:**
        i. Notify HR immediately.

ii. Perform these procedures due to the cost to the university of non-timely notifications of transfers or terminations, the risk to systems, exposure of sensitive information and negative impact on UTC's reputation should there be a compromise of any system or information.
iii. Retrieve all University system-related information and property.
iv. Disable information system access and the revoke any credentials associated with the individual.

c. **Ensure Third-Party security**. All security precautions prescribed for employee onboarding, termination and transfer must be taken when 3rd-Parties are engaged for system support.

3. Non-compliance with information security policies is addressed appropriately as in University of Tennessee Policy HR0525 - Disciplinary Action.

References:
IT0130 - Personnel Security