UT - Chattanooga: IT0115-C - UTC Standard: Information and Computer System Classification	
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 an Information & Computer System Classification 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 Information & Computer System Classification 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 Information & Computer System Classification 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. The CISO will create and maintain security procedures for the various types of classifications used by the University:
    a. Minimum Security Procedures for Devices with Sensitive Information.
    b. Minimum Security Procedures for Devices with Internal or Public Information.
    c. A security guide for the handling of physical data.
3. All system owners/administrators must:

a. Identify and document information types stored or processed by each information system.
b. Assign the appropriate classification level for data on the system.
c. Utilize the appropriate guidance provided by Information Security to protect data and systems based on their classification.

4. Classification of Data –
    a. All University data will be classified into levels of sensitivity to provide a basis for understanding and managing University data.
    b. Accurate classification provides the basis to apply an appropriate level of security to University data.
    c. These classifications of data take into account the legal protections (by statute or regulation), contractual agreements, ethical considerations, or strategic or proprietary worth.
    d. Data can also be classified as a result of the application of "prudent stewardship," where the best reason to protect the data is to reduce the possibility of harm to individuals or to the University.
5. Classification Levels –
    a. The classification level assigned to data will guide Information Owners, Information System Owners, business and technical project teams, and any others who may obtain or store data, in the security protections and access authorization mechanisms appropriate for that data.
    b. Such categorization encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated. Data is classified as one of the following:
        i. **Public** (low level of sensitivity). Public data is not considered confidential. Examples of Public data include published directory information and academic course descriptions.
        ii. **Internal** (moderate level of sensitivity). Internal data is information that is not required to be protected by law or regulation but its disclosure could be harmful or embarrassing to the University. Examples of Internal data include purchasing data, financial transactions (that do not include sensitive data), and information covered by non-disclosure agreements.
        iii. **Sensitive** (highest level of sensitivity). Sensitive data is information that must be protected by law or regulation. Examples of Sensitive data includes information related to types of research, the Family Educational Rights and Privacy Act, the Health Insurance Portability and

Accountability Act, the Gramm–Leach–Bliley Act, and the Payment Card Industry Data Security Standard.

6. **Notes -** Certain special provisions and requirements that apply to information classification are provided to ease the interpretation and implementation process.
    a. The university, except as recognized in the Statement of Policy on Patents, Copyrights, and Licensing, retains ultimate ownership of all information.
    b. Computer systems meeting the criteria of multiple classification levels must protect the highest level of information on the system or a detailed plan must be provided detailing a clear separation of data and the protections for each classification of data on the system.
    c. All computer systems that handle, process, or store the university's information at an offsite location must adhere to this program. Contracts with third-party vendors that handle, process, or store the university's information should reflect a requirement that they acknowledge and adhere to this program.

References:

IT0115 - Information and Computer System Classification