Tennessee Technological University
Policy No. 850

Enterprise Information Security

Effective Date: January 1, 2014
Policy No: 850  
Policy Name: Enterprise Information Security Policy  
Policy Subject: Enterprise Information Security Policy  
Date Revised: January 1, 2014

I. Purpose

This policy authorizes the creation of Tennessee Technological University’s (TTU) Enterprise Information Security program.

II. Review

This policy will be reviewed every 365 days or whenever circumstances require review, whichever is earlier, by the Chief Information Security Officer with recommendations for revision presented to the Chief Information Officer and the ITC.

III. Scope

This policy shall apply to all persons and organizations using the information technology facilities and resources owned, leased or administered by TTU, including all persons employed (either as full-time, part-time or temporary employees or as independent contractors) by TTU and to all students enrolled at TTU campuses. Those provisions contained herein which apply solely to employees and independent contractors are so identified individually. Unless so identified, provisions contained herein apply equally to all persons and organizations covered by this policy.

IV. Policy

Tennessee Technological University (TTU) will maintain an Enterprise Information Security Program to protect sensitive and valuable information resources against unauthorized modification, use, destruction, or disclosure, whether accidental or deliberate.

V. Definitions

A. “TTU” – Tennessee Technological University

B. “IT resources” – Information technology resources include computers and computer time, data processing or storage functions, computer systems and services, servers, networks, printers and other input/output and connecting devices, and related computer records, programs, software, and documentation.

VI. Responsibilities

A. TTU Management
Senior management has responsibility for supporting and enabling the TTU Enterprise Information Security Program, and for reviewing and approving security practices and measures as recommended by the Chief Information Security Officer.

B. Chief Information Security Officer

The Chief Information Security Officer will have overall responsibility for the development, management, and execution of TTU’s information security program.

VII. Procedures

TTU’s Enterprise Information Security Program will specify measures to protect the confidentiality, availability, and integrity of information in any form including written, spoken, and electronic information. The program will also include the hardware and software technologies used to process, transmit, and store information.

Required steps in maintaining TTU’s information security program include:

A. Balance the degree and cost of protection with the value and sensitivity of the information, regulatory and legal obligations, and the likelihood of risk or threat.

B. Provide policies, procedures, standards, services, and technologies for maintaining the appropriate level of protection.

C. Support and comply with the Tennessee Board of Regents information security policies and requirements.

D. Ensure compliance with applicable information security laws and regulations.

E. Provide awareness and training in security responsibilities and issues to TTU faculty, staff, and students.

VIII. Interpretation

The Chief Information Security Officer has final authority to interpret the terms of this policy.

IX. Citation of authority for policy

TBR Policy 1:08:00:00; State of Tennessee Enterprise Information Security Policies