Information Security Roles and Responsibilities

Effective Date: January 1, 2014
I. Purpose
This policy assigns responsibility for implementing and following Tennessee Technological University’s Information Security Program. This policy complements and supports the compliance of Tennessee Board of Regents Policy 1:08:00:00, Section 1.A and the State of Tennessee Enterprise Information Security Policies.

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 the University including all persons employed (either as full-time, part-time or temporary employees or as independent contractors) by the University or Tennessee Board of Regents and to all students enrolled at the University, and alumni.

IV. Policy
All persons and organizations using the information technology facilities and resources owned, leased, or administered by the University shall follow and adhere to the policies defined by the TTU Enterprise Information Security Program to protect information throughout the University.

V. Definitions
A. TTU – Tennessee Technological University

B. University – Tennessee Technological University

C. Information technology facilities and resources – all desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches, hubs, and mobile devices (computing platforms) owned by the University where lawfully permitted;
any computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the University’s enterprise computing or telecommunications network;

all data, information, knowledge, documents, presentations, databases or other information resource stored on the University’s computing platforms and/or transferred by the University’s enterprise network.

VI. Roles and Responsibilities

A. TTU Management - Senior management has responsibility for supporting and enabling the TTU information security program and for reviewing and approving security practices and measures as recommended by the Chief Information Security Officer. All managers and department heads are responsible for protecting information within their assigned areas of control. They are responsible for ensuring that approved protection policies, standards, and procedures are followed. They are also responsible for recognizing and reporting security vulnerabilities and ensuring that appropriate measures are implemented to address them.

B. Chief Information Security Officer - The Chief Information Security Officer (CISO) is responsible for definition, management, and execution of TTU’s information security strategy, program, and controls. The Chief Information Security Officer works closely with management throughout the University in defining security practices and measures to:

1. Identify and assess information security risks
2. Define security strategy and direction to address defined risks
3. Implement and enforce policies, procedures, and standards
4. Implement and maintain appropriate security practices and measures
5. Implement and maintain information security awareness and training program
6. Direct the response to security incidents and threats to minimize impact to the University
7. Provide consulting and assistance as needed for unanticipated information security issues
8. Perform continuous monitoring of information security program for effectiveness
C. **Information Technology Committee (ITC) of Tennessee Technological University** - The Information Technology Committee (ITC) is responsible for providing input and advice to the Information Security Office on planned policies, activities, security solutions, and security risks. The ITC will review proposed initiatives, provide counsel related to their areas of responsibility, review and approve any University policy regarding information technology, and help ensure that all areas of the University are represented in evaluation of risks and security measures.

D. **Information Technology Services** - Personnel in Information Technology Services (ITS) are responsible for maintaining a secure processing environment for the University. Working with the CISO, ITS personnel will implement security tools and practices consistent with defined strategy, and to address identified security risks. They also share responsibility for on-going monitoring and assessment to recognize new security vulnerabilities and risks.

E. **Information Owners** - An information owner refers to the person who has the ultimate authority and accountability for the information assets in his/her functional area, often a senior management person such as the head of the business function or department. An information owner is responsible for specific steps in the protection of the information resources to which he or she is assigned ownership in addition to any general management responsibilities described above. Ownership is usually designated to the functional area where the data originates or that is the primary user of the data.

Information owners’ responsibilities include:

1. Classifying information
2. Ensuring that appropriate protection measures are in place
3. Authorizing access to information
4. Ensuring compliance with policies, standards, and procedures
5. Business Continuity Planning

Information security and ITS personnel will provide assistance and tools to support these requirements. The information owner may delegate specific tasks associated with these responsibilities, such as authorizing access to information, to appropriate persons in his/her area, but may not delegate the responsibility.

F. **Information Security and ITS Support Personnel** - TTU information security personnel, ITS System Administrators, and other ITS support personnel are the
direct link between information security policies and the network, systems, and data. Specific responsibilities of these personnel include:

1. Enforce TTU information security policies and procedures as applicable to all information assets
2. Administer user account and authentication management throughout the University except for those systems where access and authentication has been delegated to system support personnel.
3. Administer and enforce TTU access control policies
4. Maintain secure processing and infrastructure equipment configurations
5. Assist in response to security incidents and threats
6. Perform the day-to-day function of information custodian

Due to the nature of their jobs, these employees may have elevated access privileges (such as system administrators in ITS) or may have access to highly sensitive data. These situations require a higher level of trust and a higher expectation of integrity. These users must not misuse or abuse their access capabilities in any way. Accessing or altering TTU data or resources, unless authorized for their specific job tasks, is prohibited.

G. All Information Users - Everyone that uses or has access to TTU information assets must recognize his/her responsibility for the safekeeping of those assets. Users must guard against abuses that disrupt or threaten the viability of all systems. All employees are expected and required to use TTU computing resources only for legitimate purposes related to their job responsibilities. The following are specific responsibilities of all TTU users:

1. Maintain awareness of and comply with the contents of all information security policies.
2. Immediately report any suspected security breach to the ITS Service Desk.
3. Handle all data and information resources with the appropriate level of security, consistent with data classification requirements, including exercising great care to maintain confidentiality of sensitive information.
4. Understand the consequences of actions with regard to computing security practices and act accordingly.
5. Use strong passwords, never share them, and maintain their security and confidentiality.

6. Always secure sensitive hardcopy documents under lock and key

7. Always lock computer screens (desktop or laptop) when left unattended, even if for only a few minutes

The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users. Persons in violation of this policy are subject to a range of sanctions (determined and enforced by TTU management), including the loss of computer network access privileges, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined in local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

VII. Interpretation

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

VIII. Citation of authority for policy

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