Information Technology Security Strategy

I. Executive Summary
The University of Tennessee, a statewide system of higher education, has four campuses, three institutes, and a presence in each of Tennessee's ninety-five counties. This distributed presence creates additional requirements for the electronic exchange of information. The university’s mission is to provide education, research, and community service to business and industry, schools, governments, organizations, and citizens throughout the state. Providing a secure and robust information technology (IT) infrastructure that supports this mission is critical. Each campus and institute plays a unique role in the overall success of the university. The university’s governance model, characterized as “distinct-but-linked”, has led to a combination of centralized and distributed management and operation of its IT infrastructure. This distributed environment presents many unique security challenges, many of which can only be addressed through centralized coordination and the collaboration of a broad statewide constituency.

The Information Security Office (ISO), under the direction of the Senior Vice President and Chief Financial Officer, has the authority and responsibility for the university’s IT security program, which includes:

- The development of a sound IT security strategy
- The development of IT security policies and adoption of best practices
- Oversight and regulatory compliance across the entire university
- Vulnerability assessment and remediation
- Incident response
- Network and systems monitoring
- Forensic analysis
- IT security consulting
- Policy and best practice compliance
- Information systems awareness training
- Business continuity

II. Scope
An effective and efficient IT security program requires the cooperation and collaboration of the entire university-wide community; therefore, this IT security strategy applies to the entire university, including all campuses and institutes. The University of Tennessee bears the responsibility for taking steps to protect the confidentiality, integrity, and availability of information in its custody, whether in electronic or material form.

III. Foundational Principles
This strategy is guided by the foundational principles of confidentiality, integrity, and availability as it relates to information and IT resources.
Confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of electronic information (i.e., has the information been released to the public without authorization?).

Integrity attempts to prevent the intentional or unintentional unauthorized modification of electronic information (i.e., has the information been altered?).

Availability attempts to insure the reliable and timely access to electronic information or computing resources (i.e., is access to the electronic information efficient and available to the person in need?).

In order to maintain confidentiality, integrity, and availability, there are a set of programs that must be established. These include:

1. A program to develop policies and adopt best practices – ensures that the university community has a standard methodology for IT security. Included in this program is a clear definition of the roles and responsibilities for all constituents.

2. A network and systems monitoring program – ensures that the infrastructure is watched for attacks.

3. A sound risk analysis and management program including a vulnerability assessment process that represents specific areas of security focus – ensures that risks and consequences are identified, evaluated, and analyzed to avoid unnecessary remediation and expenses.

4. A program to direct regulatory compliance with all federal and state laws, university policies, university best practices, and other industry regulations – assist the university in maintaining a compliant reputation with the regulatory bodies.

5. A user awareness and education program – Recognizes the importance of the human aspect of IT security.

6. A business continuity program – ensures the availability of computing and other resources necessary to carry on the mission of the university in times of physical duress.

7. An incident response program that includes forensic analysis – ensures that the proper methods for handling IT security incidents are followed and that evidence is preserved.

8. An IT security consulting program – ensures that the university user community has access to the information it needs to establish a secure IT environment.
IV. Functional Principles
In order to extend beyond the foundational principles and implement a sound IT security program there are a set of functional principles that must be applied to all IT configurations. The two principles include the following:

1. The principle of least privilege – requires that a user on a computer system be given no more privilege than necessary to perform a specific function. Implementing least privilege requires identifying the minimum set of privileges required to perform that function, and restricting the user or computer system to those privileges and nothing more.

2. The principle of defense-in-depth – requires using a layered approach to security such that single points of failure in protection are minimized. A defense in depth strategy combines people, administration, and technology to establish multiple layers of protection.

a. The People Strategy is defined as user awareness, user training, and user accountability including training efforts for students, faculty, staff, and others including but not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.

b. The Administration Strategy is defined as the policies and best practices that detail what to do and how to do it as well as the consequences of non-compliance.

c. The Technology Strategy is defined as the tools and equipment that protect the IT infrastructure.

The Foundational and Functional Principles defined in sections III and IV will be implemented using information and system classification criteria. These criteria define a framework for categorizing information according to the perceived risk to the university and assign the responsibility to the custodian to identify and designate the classification.

V. Roles and Responsibilities
All members of the university have a role in the development, implementation, and maintenance of the IT security program. For the program to be successful, it is important to establish the key roles for the personnel that will implement and maintain it. The definition of roles in the IT security program is based on industry standards as well as the model created by organizations that require the strongest IT security: the Department of Energy (DOE) and the Department of Defense (DOD). The DOE and DOD design establishes an autonomous security department that oversees all IT activities that relate to security and validates that the implementations by departments meet the IT security requirements. The
matrix showing the breakdown of the responsibilities for IT security can be found at http://security.tennessee.edu/.

**Senior Vice President and Chief Financial Officer** — Responsible for providing system oversight of all IT resources. In concert with the Executive Vice President of the university, provides the final approval for all IT policies university-wide.

**Information Security Office** — Responsible for centralized coordination and oversight of the university’s IT security. The ISO will perform both proactive and reactive IT security activities. The proactive activities include, but are not limited to, best practices definition, departmental, system, and application vulnerability assessment, firewall design review, procurement review, systems and applications design review, and policy and best practices compliance validation. The reactive activities include, but are not limited to, network and systems anomaly monitoring, forensics, and incident response as it relates to issues with critical systems or confidential information. The ISO will provide oversight and develop policies and best practices, whereas, individual campus/institute leadership will be responsible for the actual implementation.

**Campus/Institute Leadership** — Responsible for the implementation and maintenance of the protective measures required for creating a secure IT environment at the campus/institute. The secure IT environment will be based on the IT security policies and best practices as defined by the ISO. Implementation will include both proactive and reactive IT security activities. Responsible for assigning the Position of Authority for Information Systems who is the person assigned the information systems authority for that respective location.

**Information/System Custodian** — An employee acting on the behalf of the university who bears responsibility for a particular set of the university's information or a specific university system that is under their control.

**Information/System Manager** — The person or persons who have been delegated by the information/system custodian with the responsibility for maintaining security controls.

**Users** — Responsible for the implementation and maintenance of protection measures for the systems they manage based on the IT security policies and best practices.

**VI. Policies and Best Practices**
All University of Tennessee IT policies must be followed and are located at http://www.tennessee.edu/policy/. The IT security policies are created by the ISO in coordination with the Information Technology Security Council (ITSC). The Information Security Officer (ISO) chairs the ITSC with membership from the Knoxville campus, the Chattanooga campus, the Martin campus, the Health
Sciences Center, the Space Institute, the Institute of Agriculture, and the Institute for Public Service. All policies are reviewed by the Policy Management Committee and presented to the Senior Vice President and Chief Financial Officer and Executive Vice President for joint approval.

The ISO will also develop IT security best practices that provide specific guidance in protecting information and systems. The best practices are designed to establish the minimum protections necessary based on the classification of the system and the classification of the information contained on the system. These best practices must be followed unless an exception is documented and approved. Best practice documents are referenced from the Information Security Office home page at http://security.tennessee.edu/.

VII. Communications
Establishing and maintaining effective and efficient communications channels for IT security related activity is essential. To facilitate the necessary collaboration between the ISO and various system/campus/institute leaders, the ISO will establish and maintain the following IT security committees:

1. The Information Technology Security Council (ITSC) – As defined above, will assist in the development of IT security policies.

2. IT Security Technical Review Committee – Made up of representatives from the campus or institute IT technical community, this committee will assist in the implementation of best practices at the campus/institute level.

3. IT Security Business and Operations Review Committee – Made up of representatives from the campus or institute business and operations community, this committee will examine and make recommendations concerning the protocols that relate to IT security issues at the campus/institute level.

While this strategy seeks to provide clear lines of separation and segregation of duties in the assigned IT security responsibilities as defined in section V, areas of overlap will occasionally occur. In those cases, the ISO and the campuses/institutes must work together to ensure that proper security practices are implemented (e.g., incident response of critical systems or systems with confidential information, systems and applications design, and firewall design). In these areas of overlap, the ISO will fulfill its responsibility for IT security oversight. The ISO may also, at the direction of the Senior Vice President and Chief Financial Officer or at the request of campus/institute leadership, assume temporary responsibility for specific projects or security activities as necessary.

From time to time, critical IT security issues require immediate decisions by the university leadership in order to minimize risk or impact. The ISO will establish a direct line of communication with the campus, institute, or system senior leadership in dealing with these issues.
VIII. University Provided Security Resources
The university supports the need for tools for implementing sound IT security practices at campuses and institutes and will fund the “base cost” of these tools. The campuses and institutes will be provided the opportunity to buy from a university contract based on a per-unit cost. Examples of such tools include, but are not limited to, a software firewall, an encryption tool for individual files, sanitization tools, a search tool for confidential footprints, and a server change monitoring tool.

IX. Compliance
Individual areas (e.g. campuses or institutes, departments, colleges and divisions) within the university may define specific IT security requirements, guidelines, and standards as long as the documents do not detract from the university’s Information Technology Security Strategy, policies, or best practices. The university’s Information Technology Security Strategy, policies, and best practices will supersede such documents where inconsistencies exist.

Any non-compliance of the university’s Information Technology Security Strategy, policies, or best practices must be reported to the ISO. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. The ISO will work with University Human Resources and campus Student Judicial Affairs departments to develop and implement appropriate sanctions for non-compliance of the University’s Information Technology Security Strategy, policies, or best practices. Non-compliance issues that cannot be resolved by the ISO will be directed to the Senior Vice President and Chief Financial Officer. Critical non-compliance issues will be directed to the Audit Committee of the Board of Trustees.

X. Exceptions
Policies and best practices are management instructions indicating a course of action. Compliance with the university’s Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. To provide for “a standard way of doing non-standard things”, the university will implement a process for reviewing and approving/disapproving requests for exceptions. This process shall be created and maintained by the ISO for the University of Tennessee. Instructions for requesting an exception can be found at http://security.tennessee.edu/.