THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0133 - Security Planning	
Version: 1	**Effective Date: 10/01/2017**

IT0133 - Security Planning

Objective:

To establish a policy for security planning and provide the minimum requirements for plan creation, implementation, and maintenance.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

System-wide Policy: IT0133 - Security Planning	
Version: 1	**Effective Date: 10/01/2017**

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University IT resources.

Policy:

Each of the University's Campuses must develop or adopt and adhere to a formal, documented program to ensure that Security Plans providing an overview of security requirements and the controls to address those requirements are in place for critical information systems.

All policy related standards and procedures must be consistent with applicable laws, regulations, and guidance. This policy and all associated standards and procedures as well as their implementation effectiveness must be reviewed periodically and updated as needed

Mandatory Controls:

Mandatory security controls for information systems are University-wide controls that are required to be consistently designed, implemented, monitored, and assessed by all Campuses.

1. **Policy and Procedures** (PL-1): Each Campus must develop or adopt and maintain a security planning program that includes the implementation of this policy and associated controls, and an annual review of that program.

2. **System Security Plan** (PL-2): Each Campus must develop and implement a security plan for critical information systems that proves an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements.
3. **System Security Plan Update** (PL-3): System Security Plans should be reviewed at least annually and revised as needed.
4. **Rules of Behavior** (PL-4): Each Campus must ensure that all critical information system users are appropriately informed of their responsibilities and expected behavior with regard to information and information system usage. Where appropriate, the Campus should receive signed acknowledgement from users indicating they have read, understand, and agree to abide by the rules before authorizing access to the information system and annually thereafter.

Discretionary Controls:

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

References:

1. NIST 800-53 "*Recommended Security Controls for Federal Information Systems and Organizations*"

Definitions: n/a

Last Reviewed: July 17, 2017