THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0121 - Information Security Plan Creation, Implementation, and Maintenance	
Version: 2	Effective Date: 10/01/2017

IIT0121 - Information Security Plan Creation, Implementation, and Maintenance

Objective:

To establish policy for developing and maintaining an information security program at The University of Tennessee.

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.

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.

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:

1. General Policy
    a. The University IT Security Community of Practice shall create information technology (IT) security policies that provide guidance to the campuses on the implementation of an IT security program based on the National Institute of Standards and Technology (NIST) Risk Management Framework.
    b. Each campus and institute is responsible for creating, approving, maintaining, and implementing:
        i. An information security plan based on the National Institute of Standards and Technology (NIST) Risk Management Framework.
        ii. Procedures, plans, and guidelines that document the implementation strategies and steps for compliance with university policy.
    c. Each campus information security plan and documented procedures shall contain the following at a minimum:
        i. Identification and assignment of related security responsibilities including who is responsible for accepting risk at each campus and institute.
        ii. A description of the baseline controls in place or planned for meeting the security requirements.
        iii. Interconnecting systems and related Interconnection Security Agreements (ISAs).
        iv. Campus senior management approval.

   d. Each campus shall periodically review its information security plan and documented procedures based on the risk and classification of the information and/or system.
   e. A documented implementation strategy must accompany each campus information security plan including elements such as scope, timelines of implementation, risk evaluation, and a clear explanation of the proposed information and system categorization process.
2. Exceptions
   a. Requests for exceptions to system IT Security Policies must be submitted in writing to the campus Chief Information Officer or their designee, who will approve or deny the request for an exception.
   b. All exceptions must be kept on file with the Chief Information Officer or their designee.
3. Review
   a. All IT Security policies must be reviewed at least annually and approved by the IT Security Community of Practice.

Note: The data breach notification requirements are defined in the Security Incident Reporting and Response Policy.

References:

1. NIST 800-53 “Recommended Security Controls for Federal Information Systems and Organizations”

Last Reviewed: January 13, 2016