THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0124 - Risk Assessment	
Version: 2	**Effective Date: 10/01/2017**

IT0124 - Risk Assessment

Objective:

To establish policy for developing and maintaining a Risk Assessment program to ensure compliance with minimally acceptable system configuration requirements.

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.

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 that ensures the implementation of appropriate and effective system Risk Assessment (RA) controls for information systems that host or contain sensitive University information.

Mandatory controls:

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

Risk management is an information systems lifecycle approach and not a single point of time evaluation. It is the responsibility of the information system and/or information owner to ensure risk is managed. All Campus Risk Assessment programs must include:

1. **Security Categorization** (RA-2)**:** Each Campus must categorize systems and information in accordance with *University Policy IT0115, Classification*, document the categorization and review security categorization bi-annually.
2. **Risk Assessment** (RA-3)**:** Each Campus must:

a. Conduct an assessment of risk, including the likelihood and impact of identified risks to the confidentiality, integrity, or availability of information and the information systems that process, store, or transmit that information;
b. Update the risk assessment annually or whenever there are significant changes to critical information systems or their operational environment including new threats and vulnerabilities.
c. Document and disseminate risk assessment results to appropriate management and system and information custodians;

3. **Vulnerability Scanning** (RA-5): Each Campuses must:
   a. Scan critical systems and applications for vulnerabilities at least annually. Systems that require more frequent vulnerability scanning due to their risk profile or in order to comply with federal, state, or institutional regulations must be scanned accordingly.
   b. Employ industry standard vulnerability scanning tools and techniques for:
      1. Enumerating platforms, software flaws, and improper configurations;
      2. Formatting checklists and test procedures; and
      3. Measuring vulnerability impact;
   c. Remediate legitimate vulnerabilities in accordance with an organizational risk requirements.

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:

1. **Risk** – Risk is a threat and a vulnerability that may result in unwanted loss of assets or delays to normal business operations.
2. **Information Technology (IT) Risk Assessment** – The process of identifying and measuring the factors that could negatively affect the security of information technology resources.

Last Reviewed: January 11, 2017