THE UNIVERSITY OF TENNESSEE

| System-wide Policy:<br>IT0131 - Security Assessment and Authorization | |
|---|---|
| **Version: 1** | **Effective Date: 10/01/2017** |

# IT0131 - Security Assessment and Authorization

**Objective:**

To establish policy for developing and maintaining an information security assessment and authorization policy.

**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:**

Each of the University's Campuses must develop or adopt and adhere to a formal, documented program to manage the confidentiality, integrity, and availability of their critical information systems.

This program must periodically assess the security controls of information systems to determine if the controls are adequate and implemented effectively; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities of information systems; authorize the operation of information systems and any associated information system connections; and monitor information system security controls on a continuous basis to ensure continued effectiveness of the controls.

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 are University-wide controls that are required to be consistently designed, implemented, and monitored, and assessed by all campuses. Each campus or institute must establish and maintain a Security Assessment Program for all business-critical systems that includes:

1. **Security Assessment Plan** (CA-2): Each campus must develop, document, and maintain a security assessment plan that:
   a. Describes the scope of assessment including security controls and any control enhancements under assessment, assessment procedures, and assessment environment;
   b. Defines the frequency of the assessment of security controls to determine the effectiveness of implemented controls; and
   c. Produces a security assessment report and provides the results of the assessment to the Position of Authority.
2. **System Interconnections** (CA-3): Each campus must authorize, document and perform an annual review and updates of systems interconnections and Interconnection Security Agreements.
   a. Determine the types of changes to the information systems that are configuration-controlled;
   b. Review, approve/disapprove proposed configuration-controlled changes with consideration for security impact;
   c. Document configuration change decisions;
   d. Implement approved configuration-controlled changes to the information system;
   e. Retain records of configuration-controlled changes;
   f. Review activities associated with configuration-controlled changes to the information system; and
   g. Coordinate and provide oversight for configuration change control activities through a change control element that convenes regularly.
3. **Plan of Action and Milestones** (CA-5): Each campus must develop and maintain updates to a plan of action and milestones for critical systems, and document planned remedial actions to correct system deficiencies noted during assessments and continuous monitoring activities.
4. **Continuous Monitoring** (CA-7): Each campus must develop and maintain continuous monitoring program for critical systems, and document:
   a. Criteria and metrics for monitoring;
   b. Periodic assessment of monitoring criteria;

c. Monitoring and reporting of system status;
d. Response to monitoring results; and
e. Reporting.

**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.

**References:**

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

**Last Reviewed:** January 11, 2017