THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0135 - System and Information Integrity	
Version: 1	**Effective Date: 10/01/2017**

IT0135 - System and Information Integrity

Objective:

To establish policy for developing and maintaining a Systems & Information Integrity 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 to ensure the regular and timely maintenance of critical information systems, and provide effective control of that maintenance.

The program must ensure that reasonable measures are in place to protect critical information systems from threats posed by malware and other malicious or unauthorized activity; and that information system flaws are identified and addressed in timely manner.

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. All campuses must develop and maintain a system and information integrity program for critical information systems that includes:

1. **Policy and Procedures** (SI-1): Each campus must develop or adopt and maintain a System and Information Integrity program that includes the implementation of this policy and associated controls, and an annual review of that program.
2. **Flaw Remediation** (SI-2): Each Campus must:
   a. Regularly assess critical information systems for flaws and address identified issues in a timely manner.
   b. Apply relevant software and firmware updates at the earliest appropriate maintenance cycle. Critical flaws may require an emergency update between normal maintenance cycles.
   c. Incorporate flaw remediation into the organizational configuration management process.
3. **Malicious Code Protection** (SI-3): Each Campus must:
   a. Employ malicious code protection mechanisms to detect, block, quarantine, or eradicate malicious code, and alert administrative staff.
   b. Ensure malicious code protection mechanisms are current.
   c. Periodically scan critical information systems for malicious code.
4. **Information System Monitoring** (SI-4): Each Campus must:
   a. Monitor critical systems and networks for indicators of attacks, and unauthorized connections to critical information systems.
   b. Assess identified indicators and report unauthorized activity to the Position of Authority and information system owner.
   c. Ensure the integrity of monitoring tools and the information obtained from those tools.
5. **Spam Protection** (SI-8): Each Campus must employ and maintain spam protection mechanisms.
6. **Information Handling and Retention** (SI-12): Each Campus must handle and retain the output of critical information systems in accordance with applicable federal and state laws, and University policies, standards, and 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. **Flaw Remediation** - Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.
2. **Malicious Code** - Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography.

Last Reviewed: July 17, 2017