THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0135-M - System and Information Integrity Program	
Version: 6	Effective Date: 08/01/2023

Objective:

To establish and maintain a System and Information Integrity program that ensures the regular and timely maintenance of critical information systems.

Scope:

This program applies to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its remote centers.

"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 and Technology (NIST) 800 series of publications. This program is based on controls in *NIST Special Publication 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations*.

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and 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 resources.

UT - Martin Policy: IT0135-M - System and Information Integrity Program	
Version: 6	Effective Date: 08/01/2023

Program Details:

This program establishes reasonable measures to help protect critical information systems from threats posed by malware and other malicious or unauthorized activity by ensuring 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 program and all associated standards and procedures as well as their implementation effectiveness must be reviewed periodically and updated as needed (SI-1).

Roles and Responsibilities:

Chief Information Officer: Has overall accountability of this System and Information Integrity Program as the Position of Authority.

Director of IT Infrastructure: Responsible for the development, maintenance, and execution of this program.

IT Security Administrator: Responsible for:

- Managing the vulnerability scans for the campus,
- Ensuring all production servers are scanned each month,
- Making vulnerability scan results available to system administrators within a reasonable amount of time,
- Verifying vulnerability remediation and regular security patching of servers, and
- Notifying the Director of IT Infrastructure of any discrepancies in flaw remediation or security patching.

System Administrators: Responsible for installing security patches regularly to resolve critical vulnerabilities.

Vulnerability Management Scheduling:

Vulnerability scans are run on the first Sunday of each month and every Wednesday.

Flaw Remediation / Patch Management:

- Vulnerabilities that are level 4 and higher should be remediated during the scheduled maintenance window each month (SI-2). Vulnerabilities level 3 and lower should be investigated and corrected at the system administrator's discretion. Critical vulnerabilities may require an emergency update outside the regular maintenance window.
- Security patching and vulnerability remediation are to be performed during the regular maintenance window each month unless exempted by software requirements and/or server criticality.
    - Automatic updates can be setup on non-critical systems.
- Patches should be installed outside normal business hours unless it will not impact access to services or resources used by the campus.

Overview for Microsoft Windows:

Security patches for servers are downloaded and distributed by the Microsoft System Center Configuration Manager (SCCM).

Overview for Linux Distributions:

Security patches should be installed using the recommended method for the specific Linux distribution or system.

Overview for Firewall and Networking Equipment:

Security patches should be installed as critical vulnerabilities are discovered or when additional features are required.

Exceptions:

- For cases where vendors verify updates to be installed on hosts running specific software, they can be exempted from the standard patch schedule. Any exemptions need to be approved by the Security Administrator and recorded with supporting documentation.
    - Exceptions apply only to the standard patch install schedule and are not exemptions from regular patching and vulnerability remediation.
- High criticality servers (e.g., Banner) where downtime needs to be scheduled and communicated to the campus can follow a specialized patching schedule determined by the system administrator.
- If "patch day" falls on or close to important dates (e.g., class registration, first day of classes, finals, midterms, etc.), the Director of System Administration and Security can postpone patches for that month.

Malicious Code Protection:

All servers and workstations must have anti-malware applications installed (SI-3). When possible, the use of Microsoft Defender managed by SCCM should be used.

Information System Monitoring:

Critical systems and networks must be monitored for attack indicators and unauthorized connections. Any unauthorized activity must be assessed and reported to the Position of Authority and the system owner (SI-4).

Spam Protection:

ITS must employ and maintain the use of spam protection mechanisms, both incoming and outgoing, on all email platforms used by campus (SI-8).

Information Handling and Retention:

The output of critical information systems must be handled and retained in accordance with applicable laws, regulations, University policies, standards, and requirements (SI-12).

UT - Martin Policy: IT0135-M - System and Information Integrity Program	
Version: 6	Effective Date: 08/01/2023

References:

IT0135 - System and Information Integrity

IT0124 - Risk Assessment

NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations

NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology

Definitions:

Flaw Remediation - Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.

Host - A computer or IT device (e.g., router, switch, gateway, firewall). Host is synonymous with the less formal definition of system.

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.

Patch - An additional piece of code developed to address or correct security and functionality problems in software and firmware.

Patch management - The process for identifying, acquiring, installing, and verifying patches for products and systems.

Remediation - The act of correcting a vulnerability or eliminating a threat by installing a patch, adjusting configuration settings, or uninstalling a software application.

Spam - Unsolicited bulk email messages.

System Administrator - A person who manages the technical aspects of a server / system.

Vulnerability - A flaw in the design or configuration of software that has security implications.