

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

Objective

To establish a program for developing and maintaining a Systems & Information Integrity program to ensure compliance with minimally acceptable system configuration requirements.

Scope

This plan applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee Space Institute (UTSI) 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, 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.

UTSI must develop or adopt and adhere to a plan that demonstrates compliance with related policies and standards. This plan 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 University policy is assumed if a User accesses, uses, or handles University resources.

Roles and Responsibilities

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

IT Administrator: Responsible for conducting vulnerability scanning for all systems on campus.

Program Details

UTSI 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.

This 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.

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

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).

Vulnerability Management

- It is the responsibility of the IT Administrator to:
 - Manage the vulnerability scans for the campus,
 - Ensure all production systems are scanned each month,
- Vulnerability scans are performed regularly using systems provided by the University of Tennessee System Administration Information Security Office (UTSA ISO) (RA-5).
 - Other systems may be used to enhance or complement this system.

Scheduling

Vulnerability scans are run quarterly on the first day of every third month.

Flaw Remediation / Patch Management

- Vulnerabilities that are level 5 and higher must be remediated quarterly (SI-2). Vulnerabilities level 4 and lower should be investigated and corrected at the IT administrator's discretion. Critical vulnerabilities may require an emergency update outside the regular maintenance window.
- References to patches and/or steps taken by IT administrators to resolve vulnerabilities must be documented in the IT helpdesk ticket system.
- It is the responsibility of system administrators to ensure security patches are installed regularly to resolve critical vulnerabilities.
- Security patching and vulnerability remediation are to be performed on or around the first day of each month unless exempted by software requirements and/or server criticality
 - Automatic updates can be setup on non-critical systems.

Overview for Microsoft Windows

- Security patches for servers are downloaded to SCCM every day.
- Security patches for servers are to be installed on or around the first day of each month.
 - Patches should be installed outside normal business hours unless it will not impact access to services or resources used by the campus.
- Security patches for workstations are distributed automatically by SCCM using Automatic Deployment Rules.

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

Overview for Linux Distributions

Security patches are downloaded and installed on or around the first day of each month.

Overview for Firewall and Networking Equipment

Security patches are downloaded and installed quarterly on or around the first day of every third month.

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 IT 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 (ex. Domain controllers, Exchange) where downtime needs to be scheduled and communicated to the campus can follow a specialized patching schedule determined by the IT administrator.
- If “patch day” falls on or close to important dates (ex. class registration, first day of classes, finals, midterms, etc.), the CIO or IT Administrator can postpone patches for that month.

Compliance

The IT Administrator is responsible for verifying vulnerability remediation and regular security patching of servers. The CIO will be notified of any discrepancies in flaw remediation or security patching and will communicate those to the appropriate party.

Malicious Code Protection

All servers and workstations must have anti-malware applications installed (SI-3). When possible, the use of Microsoft System Center Endpoint Protection managed by System Center Configuration Manager 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

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

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

Information Handling and Retention

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

Mandatory Controls

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

- 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.
- Flaw Remediation (SI-2). Each Campus must:
 - Regularly assess critical information systems for flaws and address identified issues in a timely manner.
 - Apply relevant software and firmware updates at the earliest appropriate maintenance cycle. Critical flaws may require an emergency update between normal maintenance cycles.
 - Incorporate flaw remediation into the organizational configuration management process.
- Malicious Code Protection (SI-3). Each Campus must:
 - Employ malicious code protection mechanisms to detect, block, quarantine, or eradicate malicious code, and alert administrative staff.
 - Ensure malicious code protection mechanisms are current.
 - Periodically scan critical information systems for malicious code.
- Information System Monitoring (SI-4). Each Campus must:
 - Monitor critical systems and networks for indicators of attacks, and unauthorized connections to critical information systems.
 - Assess identified indicators and report unauthorized activity to the Position of Authority and information system owner.
 - Ensure the integrity of monitoring tools and the information obtained from those tools.
- Spam Protection (SI-8). Each Campus must employ and maintain spam protection mechanisms.
- 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.



SPACE INSTITUTE

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

- **Vulnerability Scanning (RA-5).** Requires that UTSI:
 - 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.
 - Employ industry standard vulnerability scanning tools and techniques for:
 - Enumerating platforms, software flaws, and improper configurations;
 - Formatting checklists and test procedures; and
 - Measuring vulnerability impact;
 - Remediate legitimate vulnerabilities in accordance with 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

IT0135 – *System & Information Integrity Policy*

IT0124 – *Risk Assessment*

NIST 800-53 Revision 4 *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-40 Revision 3 *National Institute of Standards and Technology Guide to Enterprise Patch Management Technologies*



SPACE INSTITUTE

UT Space Institute Policy:	
IT0135-SI – System and Information Integrity Program	
Version: 1	Effective Date: 10/06/2019

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 messages sent through email.

Steganography - The practice of concealing information within another message, image, or file.

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