

UT Space Institute IT Procedure:	
Vulnerability Management, Audit Log Management, and Malware Defense Procedure	
Version: 1	Effective Date: 10/01/2025

Purpose

To establish processes for performing Vulnerability Management, for performing threat and vulnerability monitoring, for creation and maintenance of audit logs, and for installation of anti-malware software on all University Assets.

Scope

This procedure applies to University owned or managed Assets, Systems, and Resources only. It does not apply to Assets, Systems, and Resources not owned by the University unless specifically stated in the policy.

Procedure

- Vulnerability Management Procedure

All server systems are enrolled in the UT System Vulnerability Management software and scanned daily. IT Administrators review vulnerability scan results weekly and remediate any vulnerabilities found. If remediation is not possible, an exception must be submitted to UT for any high-risk vulnerabilities that remain unpatched after 14 days. This exception must include the device/application name, type of data handled, and mitigating controls that will be placed instead of patching.

Server systems are patched on a weekly basis for Windows machines and daily for Linux boxes. Applications hosted on these servers and network appliances are patched monthly. Detailed information on server patching procedures can be found at the centralized CS data store.

All client machines are patched within one week of Patch Tuesday via SCCM.

- Audit Log Management Procedure

All server systems are enrolled in Azure Arc and logs are collected and assessed through UT System.

UT Space Institute IT Procedure:	
Vulnerability Management, Audit Log Management, and Malware Defense Procedure	
Version: 1	Effective Date: 10/01/2025

Client system logs are left at the default level upon initial Windows/Linux install and accessed on the machine as needed.

The primary domain controller on the UTSI network is responsible for time synchronization. Via group policy setting, the PDC is set to sync with ntp.org time servers as well as time.microsoft.com. All other server and client machines are set via Group Policy to use the PDC, ntp.org, and time.microsoft.com as their NTP servers.

DNS logging is enabled on all external and internal servers that provide DNS services.

URL request logs are enabled and stored on the primary campus firewall.

- **Malware Defense Procedure**

All systems use Microsoft Defender for antivirus and antimalware protection. Server systems are joined to the UT System Azure Arc instance. All client systems are joined to Active Directory and automatically enrolled and managed by UTSI SCCM. Windows Defender signature updates are applied at least daily via SCCM deployment rules.

Windows Defender Endpoint Protection automatically scans removable media and uses real-time file protection for any accessed file.

Software on UTSI systems is audited inside of SCCM to ensure only currently supported software is installed.

The UTSI campus firewall provides up-to-date threat prevention, Advanced WildFire malware analysis to block unknown files and file types, URL filtering, and DNS filtering.

AutoRun and AutoPlay behavior is disabled via Group Policy.

Exceptions

Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

Related Policies



SPACE INSTITUTE

UT Space Institute IT Procedure: Vulnerability Management, Audit Log Management, and Malware Defense Procedure	
Version: 1	Effective Date: 10/01/2025

- [IT0001 – General Statement on Information Technology Policy](#)
- [IT0003 – Information Technology Security Program Strategy](#)
- [IT0004 – Information Technology Risk Management](#)
- [IT0005 – Data Categorization](#)
- [IT0014 – Information Technology Security Awareness Training Management](#)
- [IT0017 – Information Technology Incident Response Management](#)
- [IT0102 – Information Technology Asset Management](#)
- [IT0311 – Information Technology Data Access, Management, and Recovery](#)
- [IT0506 – Information Technology Account and Credential Management](#)
- [IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing](#)
- [IT1516 – Information Technology Service Provider Management and Application Software Security Management](#)
- [IT4912 – Information Technology Secure Configuration Management](#)
- [HR0580 – Code of Conduct](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)