

UT Space Institute IT Procedure:	
IT Service Provider Management and Application Software Security Management	
Version: 1	Effective Date: 10/01/2025

Purpose

To establish appropriate control mechanisms for securing the University Information Technology Networks and to create a Penetration Testing process.

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

1. Network Monitoring and Defense
 - All server and network devices utilize Azure Arc to collect event data. Alerts are generated and distributed by Dell and UT System through the monitoring of the assets added to Arc.
 - Network Intrusion Detection and Intrusion Prevention are handled by the Institute's firewall. The current Palo Alto firewall solution also offers application layer filtering which is enabled and tuned to only allow specific applications where needed.
2. Penetration Testing
 - The Institute is part of the CISA Cyber Hygiene program. This program is an external penetration test which attempts to penetrate addresses in the entire UTSI IP block as well as specific web and applications exposed to the Internet.
 - Hosts are scanned randomly between the hours of 8 p.m and 6 a.m.
 - After the initial scan, hosts are rescanned based on the following schedule
 - Addresses with no running services detected (dark space) are rescanned after at least 90 days.
 - Hosts with no vulnerabilities detected are rescanned every 7 days.
 - Hosts with low-severity vulnerabilities are rescanned every 6 days.
 - Hosts with medium-severity vulnerabilities are rescanned every 4 days.
 - Hosts with high-severity vulnerabilities are rescanned every 24 hours.
 - Hosts with critical-severity vulnerabilities are rescanned every 12 hours.
 - Reports of all vulnerabilities are provided with each rescan up to every 12 hours.
 - Vendor contact information. Email – vulnerability@mail.cisa.dhs.gov
 - UTSI IT Services are responsible for patching any high or critical vulnerabilities with 14 days as noted in IT7810.



SPACE INSTITUTE

UT Space Institute IT Procedure:	
IT Service Provider Management and Application Software Security Management	
Version: 1	Effective Date: 10/01/2025

- Security measures are to validated after each penetration test to identify areas improvable capabilities or rulesets can be implemented to detect the techniques and methods used in the testing.

Exceptions

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

Related Policies

- [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](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)
- [HR0580 – Code of Conduct](#)



SPACE INSTITUTE

UT Space Institute IT Procedure:	
IT Service Provider Management and Application Software Security Management	
Version: 1	Effective Date: 10/01/2025

- [IT4912 – Information Technology Secure Configuration Management](#)
- [IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy](#)