



SPACE INSTITUTE

UT Space Institute IT Procedure: Secure Configuration Management	
Version: 1	Effective Date: 10/01/2025

Purpose

To provide guidance and structure for the campus to create and maintain consistent processes for securely configuring 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

1. Client Configuration
 - a. The initial setup steps that cannot be automated are listed in the UTSI Initial PC Setup document stored at the centralized CS data store.
 - b. All client machines must be added to the UTSI Active Directory. Client machines that run older OS systems or that cannot be joined to Active Directory will be unable to access the network.
 - c. Active Directory Group Policy pushes security configuration to the client machines including screen time outs, password and account settings, firewall settings, and update settings.
 - d. Management of systems must be performed with accounts that have “Run As” or “sudo” rights.

2. Server Configuration
 - a. The initial setup steps, software setups, and any settings for the server machines that cannot be automated are stored in baseline documents at the centralized CS data store.
 - b. Configuration of Linux servers are done based on the baselines at the centralized CS data store.
 - c. All Windows server systems must be added to the UTSI Active Directory
 - d. Active Directory Group Policy pushes security configuration to the server machines including screen time outs, password and account settings, firewall settings, and update settings.
 - e. Specific update procedures for servers are listed in the centralized CS data store.
 - f. Management of systems must be performed with accounts that have “Run As” or “sudo” rights.



SPACE INSTITUTE

UT Space Institute IT Procedure: Secure Configuration Management	
Version: 1	Effective Date: 10/01/2025

3. Network Appliances (Switches, firewalls, wireless controllers, etc.)
 - a. The initial setup steps, software setups, and any settings for the network appliances are stored in baseline documents at the centralized CS data store.
 - b. Updates to system software, firmware, and applications these appliances are performed quarterly by IT Administrators.
 - c. Management of these appliances must be performed via secure protocol such as SSH or HTTPS.

All changes to automated processes, server setups, and network appliances are to be approved by campus CIO and documented in helpdesk tickets.

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](#)



SPACE INSTITUTE

UT Space Institute IT Procedure: Secure Configuration Management	
Version: 1	Effective Date: 10/01/2025

- [IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing](#)
- [IT1516 – Information Technology Service Provider Management and Application Software Security Management](#)
- [HR0580 – Code of Conduct](#)
- [IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy](#)
- [IT0002 – Acceptable Use of Information Technology Resources](#)