

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

Objective

To establish a formal, documented plan that describes the implementation of appropriate and effective Configuration Management (CM) controls for business-critical systems (CM-9). This plan establishes guidelines for baseline configurations and defines the change control process for managing configuration changes.

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 plan is based on those guidelines. This plan is based on guidelines in NIST Special Publication 800-128 *Guide for Security-Focused Configuration Management of Information Systems*.

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.

Plan Details

Configuration management is comprised of the various activities focused on establishing and maintaining the integrity of systems. This is accomplished through specifying and controlling the processes for initializing, changing, and monitoring the configurations of those systems.

Roles and Responsibilities

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

Chief Information Officer - Has overall accountability of this Configuration Management Plan as the Position of Authority.

System Administrators - Responsible for maintaining configuration management of the system(s) for which they administer and the development and maintenance of baselines for individual or classes of systems.

Applicable Systems

This plan applies to all IT systems under the responsibility of UTSI personnel. A list of these systems can be found in the UTSI System Classification and Risk Assessment sheet.

Baseline Configurations

When possible, baseline configuration documents will be created for each system on UTSI campus. Baseline configurations must be reviewed at least annually and will be changed as necessary (CM-2.1). N-2 baselines should be kept for audit and roll-back purposes (CM-2.3).

Least Functionality

Information systems must be configured to provide only essential capabilities and specifically prohibit or restrict unnecessary functions, ports, protocols, and services (CM-7). See Appendix A - Least Functionality Details for more information.

Configuration Change Control

Configuration Change Control refers to the documented process for controlling and managing changes to the configuration of an information system or its Configuration Items (CIs). It is applied to include changes to components of a system, configuration settings, emergency/unplanned changes, and patch installation / flaw remediation.

Overview

Most RFC procedures will follow this general format:

1. Request and Record
2. Initial Approval (Optional)
3. Assign
4. Test
5. Final Approval



SPACE INSTITUTE

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

6. Implement
7. Verify
8. Close

Request and Record

The change request is created in UTSI Helpdesk ticket system. Information requested includes:

- Description
- Risks
- Systems and/or services affected
- Roll-back plan

Initial Approvals (Optional)

The initial set of approvals is performed only for certain changes and systems.

Assign

The change request is assigned to the change implementer who is responsible for testing and implementing the proposed change. The implementer is either assigned in the UTSI Helpdesk System or informally depending on the system(s) and type of change.

Test

The requested change should be applied to the pre-production or test environments, if applicable. Roll-back procedures should also be developed as part of testing by the change implementer. If testing the change implementation fails, it will be rolled back and the RFC will either be reassigned or closed.

The Security Impact Analysis should be conducted during this phase to determine the extent to which the changes affect the security posture of the system and whether mitigating controls are needed (CM-4).

Final Approvals

Once the change has been tested, the final approvals are processed before implementation. Approvers are determined by systems for which the change is requested.

Implement

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

During change implementation, the requested and tested changes are applied to the production system(s). If the change implementation fails, the changes will be rolled back using the procedure developed during testing and the RFC is either reassigned or closed.

Verify

Once the changes have been applied, there will be a post-implementation review on the system(s) to determine if the change was applied correctly and with expected results.

Close

All changes or roll-backs have been successfully completed and the RFC status in UTSI Helpdesk ticket system is set to “Closed.”

Excluded Changes

Standard / common changes are excluded from change control when no users or services will be impacted (CM-3):

- Password resets
- Add/remove/modify user accounts or security groups
- Restarting machines when no configuration change has been made and when no users or services will be impacted
- File permission changes
- Changes to non-production systems

Type of Change

The type of change drives the workflow and approval processes along with the category, sub-category, and reason for change.

- Emergency – Change that must be completed as soon as possible
- Normal – Follows the standard change workflow

Scope of Change

The scope of change is based on the potential user impact.

- Critical - University-wide, potentially affecting all user groups (faculty, staff, students) and centers



SPACE INSTITUTE

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

- High - potentially affecting a specific campus/center
- Medium - affecting a building or department
- Low - affecting a single user

Monitoring

Where technically feasible, monitoring will be implemented on systems to detect unauthorized changes and deviations from the approved baseline configurations (CM-6).

References

IT0125 - *Configuration Management*

NIST SP 800-128 - *Guide for Security-Focused Configuration Management of Information Systems*

NIST SP 800-123 - *Guide to General Server Security*

NIST SP 800-53 Rev4 - *Recommended Security Controls for Federal Information Systems and Organizations*

Definitions

Baseline Configuration - A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The Baseline Configuration is used as a basis for future builds, releases, and/or changes.

Configuration Change Control - Process for managing changes to the Baseline Configurations for Configuration items.

Configuration Management - Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

Least Functionality - Configuring information systems to provide only essential capabilities and specifically prohibiting or restricting the use of extra functions, ports, protocols, and services.

UT Space Institute Policy: IT0125-SI – Configuration Management Plan	
Version: 1	Effective Date: 10/06/2019

Appendix A - Least Functionality Details

Systems should be configured with only the necessary services, applications, and network protocols needed to provide the function for which they are created. Open ports and protocols are at risk of reconnaissance and/or exploitation, especially when vulnerabilities exist.

Least functionality will be evaluated as part of security assessments conducted in accordance with IT0131-SI - *Security Assessment and Authorization Plan* (CM-7.1a).

Common types of services and applications that should be removed or disabled (CM-7.1b) if not required include, but are not limited to, the following:

- File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], FTP)
- Wireless networking services
- Remote control and remote access programs, particularly those that do not strongly encrypt their communications (e.g., Telnet)
- Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS])
- Web servers and services
- Email services (e.g., SMTP)
- Language compilers and libraries
- System development tools
- System and network management tools and utilities, including Simple Network Management Protocol (SNMP)

Completely removing unnecessary services is preferable to simply disabling them. Attacks that attempt to alter settings and activate a disabled service cannot succeed when the functional components are removed. This can enhance the security of the server in the following ways:

- Services cannot be compromised and used to attack the host or impair the services of the server. Each service running on a host increases the risk of compromise for that host because each service is another potential point of entry for an attacker.
- Unused services may have defects or be incompatible with the server. By removing or disabling them, they should not affect the server which could potentially improve its availability.
- The host can be configured to better suit the requirements of the particular service. Different services could require different hardware and software configurations, which could lead to unnecessary vulnerabilities or degraded performance.
- By reducing services, the number of logs and log entries is reduced so detecting unexpected behavior may become easier.