THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: CM-001-Configuration Management	
Version 1	**Effective Date: 07/18/2023**

Responsible Office: Office of Cybersecurity	Last Review: 07/18/2023 Next Review: 07/18/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To establish requirements for implementing and maintaining Configuration Management for IT Resources in order to minimize operational malfunctions, intrusions by external threats, exploitation of vulnerabilities, unauthorized data disclosures, and performance problems. Failure to protect University information systems, hardware, and networks against threats and substandard configurations can result in the loss of data integrity, unavailability of data, and/or unauthorized use of data or information systems of which University departments are considered the owner.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

The Configuration Management standard and supporting requirements apply to all information technology assets, systems, networks, and data hosts that are owned by, managed by, and/or sponsored by UTHSC. This standard is also applicable to the UTHSC workforce who own, operate, or maintain these systems for University business, academia, and research.

Definitions

Baseline Configuration – documented, formally reviewed, and agreed-upon sets of specifications that ensure that IT Resources are properly configured and hardened to reduce vulnerabilities.

Change Management – controls and communicates the changes occurring in the ITS environment.

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.

Hardening – the process of securing an IT Resource configuration and settings to eliminate as many security risks as possible to reduce vulnerability and the possibility of being compromised. Hardening may include, but is not limited to, changing default passwords, removing unnecessary software, removing unnecessary usernames or logins, and disabling or removing unnecessary services.

IT Resource – any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. applications and support systems), and information.

UTHSC Workforce – employees, volunteers, trainees, and other persons who conduct business for UTHSC, whether or not they are paid by UTHSC.

Responsibilities

Change Advisory Board (CAB) is responsible for managing the Change Management Program, ensuring that risks are accurately assessed, authorizing changes to proceed, and managing a change schedule to maximize the number of successful service and product changes.

Chief Information Security Officer (CISO) is responsible for enforcing the application of appropriate operational security controls necessary to mitigate risks associated with unauthorized disclosure, loss, or theft of university information.

System Custodian is responsible for the maintenance and operations of the technological infrastructure, including network or applications, to support running the system(s) supporting University activities. The system custodian should know the system assets and technical operations and be able to advise on the technical impact of a compromised system.

System Owner is a senior stakeholder within the University system who is responsible for ensuring that technology system functions meet University goals and adhere to University policies and standards. Working with the System Custodian, ITS Risk Management Function, and Cybersecurity Function, they should identify the potential threats to a system, conceptualize risk scenarios, and determine risk likelihood and impact.

Standard

The configuration management standard is to ensure that the University technology systems abide by a baseline configuration and have a consistent minimum-security standard in place to prevent any intrusion by external threats, exploitation of vulnerabilities, unauthorized data disclosures, and performance problems and flaws.

Any hardware asset that is in operation to collect, transmit, process, store, or host University data must be inventoried, per GP-007-Asset Management, hardened, monitored, and managed from initial installations, through configuration, maintenance, and support, to end-of-life decommissioning. Industry-approved baseline configurations or best practices are used to configure the asset to protect the confidentiality, integrity, and availability of UTHSC assets (i.e. CIS Benchmarks, OWASP, vendor whitepapers, etc.).

The higher the classification of the asset or the data associated with the asset, or the more it is viewed to be susceptible to risk or exploitation, the higher the level of protection required for its management. Classification levels are explained in GP-002-Data & System Classification.

All servers and end-user workstations that are in operation to collect, transmit, process, store, or host University data must be formatted and configured using the authorized protocols, controls, and settings sufficient to safeguard the University's systems and their associated data.

Systems must be configured to provide only essential capabilities. Non-essential services, functions, ports, protocols, etc. should be disabled or restricted.

Change Control

Configuration change control is implemented and maintained through Change Management processes. These processes are explained in this Change Management Knowledge Base (KB) article.

Failure to Comply

Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the computer and/or disciplinary action per GP-001.04 Information Security Violations for the individual violating the policy.

Policy Exceptions

Exceptions to this Standard should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. UTSA IT0125 – Configuration Management
2. Change Management KB Article
3. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
4. GP-001.04-Information Security Violations
5. GP-002-Data & System Classification
6. GP-007-Asset Management