Purpose and Benefits

Secure Configuration Management ensures the security and integrity of information technology operating systems, applications, and devices and is a crucial practice for the University of North Texas System (the System). The Secure Configuration Management Standard establishes the CIS Benchmarks™ as the System's baseline requirements for configuration management. All Information System/Application Owners and System Administrators are required to comply with the guidelines established herein concerning Secure Configuration Management.

Authority and Requirements

System Configuration Hardening and Patch Management section of the UNT System Information Security Handbook (Page 33-34). The System Configuration Hardening and Patch Management requirements of the UNT System Information Security Handbook satisfy the control requirements of CM-Configuration Management in the Texas Department of Information Resources Security Controls Standards Catalog.

Definitions

CIS Benchmarks™. "CIS Benchmarks" means consensus-based, best-practice security configuration guides developed and accepted by government, business, industry, and academia.

Configuration. "Configuration" means the possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.

Configuration Management. "Configuration Management" means a collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Information Security Program. "Information Security Program" means the policies, Information Security Handbook, control catalog, standards, procedures, trainings, strategies, objectives, resources, and plans that establish the information resources security function for the UNT System and its institutions. The Information Security Program shall comply with applicable federal and state laws related to information resources and information security, including but not limited to 1 Texas Administrative Code §202 and the State of Texas Department of Information Resources Security Controls Standards Catalog.

Information Resource/Application Owners. "Information System/Application Owners" means Custodians who are responsible for the development, procurement, integration, modification, operation and maintenance, implementation of the Information Owner-defined controls, and/or final disposition of an information resource.

System Administrators. “System Administrators” means a Custodian responsible for the installation and maintenance of an information resource, providing effective utilization, adequate security parameters, and sound implementation of established policy and procedures.

General Implementation

All IT systems must be configured in accordance with the latest CIS Benchmarks™ relevant to the specific operating system, application, or device. System administrators must regularly review and update configurations to align with the most current CIS Benchmarks™. Implementation of the CIS Benchmarks™ for operating systems, applications, and devices supports compliance with the UNT System Information Security Program.

Information Resource/application owners must identify and document the configuration items (CIs) within the information system and maintain an inventory of all CIs, including hardware, software, and network components.

System Administrators must regularly update configurations based on the latest CIS Benchmarks to address emerging threats and vulnerabilities.

System Administrators must implement automated tools to enforce and monitor compliance with CIS Benchmarks™, maintaining all documentation of all configurations, including any deviations from the CIS Benchmarks™. Deviations from the CIS Benchmarks™ must include justification and mitigating controls and may require an exception depending on severity.

Regular Assessments

System Administrators must conduct regular assessments to ensure that CIs are in compliance with CIS Benchmarks™.

Security Operations may perform vulnerability assessments and penetration testing on High Impact and Moderate Impact resources to identify and remediate any configuration weaknesses.

Configuration Change Control

Configuration changes must follow the UNT System Change Enablement Standard to ensure each change is documented, approved, and assessed for risk, impact, and security.

Incident Response

Security Incidents related to configuration issues must follow the System’s incident response plan and procedures to ensure that any deviations from CIS Benchmarks™ identified during an incident are documented and addressed promptly.

Exceptions and Compensating Controls

Exceptions to Information Security policies and this standard may be approved by the Chief Information

Security Officer or their delegate when accompanied with sufficient justification and compensating controls, in accordance with the UNT System Information Security Program.

The Chief Information Security Officer may revoke an exception at any time.

References and Notes

DIR Security Controls Standards Catalog
UNT System Information Security Regulation 06.1000
UNT System Information Security Handbook
NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems
Center for Internet Security (CIS) Benchmarks List

Approvals and Revision History

	Name	Title	Date
Authored By:	Christine Sikes	Director of IT Governance. Risk. & Compliance	5/14/2025
Approved By:	Richard Anderson	Associate Vice Chancellor and Chief Information Security Officer	10/22/2025

Date	Approved By	Version	Notes
10/22/2025	Rich Anderson	1.0	New Secure Configuration Management Standard