Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-06: Configuration Management Standard

Standard Contents

1. Purpose

The purpose of the Configuration Management Standard is to establish the enterprise requirements for managing risks by requiring common baseline standards and “hardened” configurations for endpoints, networks, and systems. The overriding goal of this standard is to reduce operating risk and facilitate regulatory compliance.

2. Scope

This standard shall apply to all The University of Nebraska (“The University”) technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this standard to establish secure configurations throughout The University to help the organization implement security best practices for Information Systems (endpoints, networks, and systems as defined in Executive Memorandum 16). Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (“CISO”) as defined in **ITS Policy Exception Standard**. The following subsections outline the Configuration Management Standard.

4. Configuration Management Requirements

4.1 Establish Configuration Baselines

4.1.1 Establish and Maintain Configuration Baselines and Inventories

Inventories of all information systems will be conducted as defined in the **Asset Management Standard**. Baseline configurations for all inventoried information systems will be an agreed-upon set of industry-accepted specifications for each target information system and/or configuration item(s) within those information systems. All configuration baselines must be documented and agreed-to by at least the service owner, system administrator, and the CISO. A centralized system for configuration baseline information repository must be established and maintained. Where possible this repository should be integrated with the change management and asset management system(s).

Hardened configuration baselines must be established, documented, and reviewed annually for all inventoried information systems.

Administrative users that need to make non-emergency information system baseline configuration changes to any information system must use the formal change control and approval process before making any information system baseline changes. Emergency baseline configuration changes made by administrative users must be documented and approved as soon as possible but no later than 3 working days of the change that took place. Approved exceptions must be periodically reviewed to ensure ongoing appropriateness and business need.

Periodic monitoring of all information systems will ensure that hardware, software, and operating systems remain compliant with established hardening standards. Identified discrepancies must be identified and remedied or request a formal exception.

4.1.2 Employ Principle of Least Functionality

Where feasible, information systems shall be designed, implemented, and configured to serve one primary function to prevent the co-existence of multiple functions requiring varying levels of security controls or hardened configurations. Information systems will be reviewed at least annually to ensure the functions and services provided by the information system and its components are required.

4.1.3 Control and Monitor User-installed Software

Only authorized software is permitted to be installed on University information systems. A formally approved list of authorized software technologies and on what information systems their use is permitted will be created and maintained. All software not on the approved list must be approved through the exception or change control processes prior to installation and use. All software requests must have a documented business purpose. The approved software list and exceptions will be reviewed annually for ongoing business need. Additionally, a blocklist of expressly unauthorized software titles or types of software will also be maintained. Software on this blocklist is never permitted for use at any time.

Non-administrative users must be prevented from installing unapproved software or making unapproved information system baseline changes. Non-administrative users can only install approved software from approved locations such as University maintained software libraries. Other unapproved software or information system baseline changes must be requested via the help center before making any information system baseline changes. Monitoring technologies will be implemented to detect and report instances of unauthorized software on University information systems.

Control and Monitor User-installed Software applies to information systems in scope with (a) federal security-related laws and regulations, (b) state and local security-related laws and regulations, and (c) contractual requirements.

4.2 Perform Configuration and Change Management

4.2.1 Establish and Enforce Security Configuration Settings

Configuration settings are parameters that can be changed in hardware, software, or firmware of the information system. Secure configurations (often called security configuration checklists, security benchmark, or hardening guides) provide recognized, standardized, and established benchmarks for securely configuring a given information system. Where possible a security configuration benchmark for the information system or software in question will be used. The chosen benchmark (and any deviations or customizations) must be clearly documented in the baseline configuration repository for each information system. Common industry-accepted security hardening standards include those defined by:

- The Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- Sysadmin, Audit, Network, and Security (SANS) Institute
- National Institute of Standards Technology (NIST)
- Product vendors (e.g. Microsoft, Cisco, etc.)

4.2.2 Physical and Logical Access Restrictions

Only qualified and authorized personnel are permitted to have access to and make physical and logical changes to the organizational hardware, software, software libraries, and/or firmware. Those personnel and their assigned responsibilities must be identified and documented. This may include:

- Physical access to controlled areas
- Logical access to information system configurations
- Manual and automated workflow and approval processes
- Manual and automated configuration management systems

4.2.3 Restrict Use of Nonessential Programs, Functions, Ports, Protocols, and Services

Baseline configurations must include the disabling of vendor supplied accounts (or, at a minimum, the changing of default passwords) and the disabling of unnecessary ports, protocols, and services according to the principle of least functionality. Only needed ports and protocols required for the information system should be permitted on the network. All unneeded ports and protocols should be blocked.

4.2.4 Track, Review, Approve or Disapprove, and Log Changes to Organizational Systems

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. This process must be systematic in its function in order to properly maintain information system baselines. A Change Advisory Board (CAB) will be established oversee this process.

4.2.5 Change Advisory Board

A CAB will be established to oversee the tracking, review, and approval of change requests. The CAB will establish procedures to ensure that all the necessary requirements to manage configuration change control properly and effectively are met. Change requests should be submitted in advance of the proposed change date and generally involves the following steps with appropriate documentation occurring at each point:

1. Proposed change request with appropriate business justification, documentation, comms plan, etc.
2. Risk assessment - Analyze the change for potential impacts, security, and availability concerns
3. Review and approval of the proposed change
4. Testing of the proposed change
5. Implementation of the change in production
6. Documentation updated and change closed

4.2.6 Change Request, Justification, and Documentation

The Change Control Manager will establish business justification and detail requirements for requested changes in order to be approved. Minor configuration changes will need less review and testing than major configuration changes (new information systems or major upgrades to existing information systems) which might require months of planning and testing. The Change Control Manager will ensure that enough time is available at each step to allow for the necessary actions to be performed and documented. Requirements and time thresholds for each change type will be established according to the change management procedures. The change request and all supporting documentation must be stored in a change management system. At a minimum, the change record must include:

- Change classification, in alignment with Change Management procedures
- Details of the change
- Date and time of proposed implementation
- Business justification and risk assessment
- Directly and indirectly affected service(s)
- Individual responsible for implementing the change
- Backout or contingency plan
- Test plan (or rationale for why testing is not possible)
- Validation plan

4.2.7 Risk Assessment and Security Impact Review

Change and system owners should analyze changes to their systems to determine potential security and availability impacts prior to change implementation. These impacts should be documented in the change request.

The CISO will appoint a team to conduct a security impact analysis on each proposed change ahead of the CAB meetings. There should be enough time to review the change and document any risks. This analysis should include reviewing the proposed change, security plans, security requirements, information system design, and information system documentation. Identified compromise of security controls, risks, and/or adverse impacts to the system or network must be addressed or mitigated prior to implementation into production environments.

4.2.8 Review and Approval

Change requests must be reviewed and approved by the majority of CAB members to be approved. Separation of duties must be enforced between development, testing, implementation, and approver personnel. When separation of duties cannot be enforced, change monitoring controls must be in place to validate the appropriateness of each change.

4.2.9 Change Testing

Changes must have a documented test plan to confirm changes are implemented in a controlled manner. Test plans may include test scripts, input data, expected results, actual results, verification of key controls, and user acceptance testing. Testing requirements must correlate with the complexity of the change. Where technically feasible, changes to infrastructure must be tested in a non-production environment. The use of production data in a test environment is discouraged. Production data may only be used in test and non-production environments in either of the following circumstances:

- The non-production environment has been authorized as having the same appropriate level of security control as the production environment
- Production data has been sanitized or anonymized in a manner that has rendered production data unrecognizable and impossible to reconstruct

4.2.10 Change Implementation
Access to implement changes in the production environment must be limited to authorized users in accordance with job responsibilities and in alignment with the Access, Identification and Authorization Standard.

4.2.11 Documentation
Once the change is complete, the test results, implementation results, and information system baseline configuration information must be documented and stored in the change management and/or baseline configuration management system(s).

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published