UNIVERSITY OF

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 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 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

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

4.2.10