Effective: *September 19, 2017*
Last Revised: *March 27, 2019*

Responsible University Administrators:
Vice President for Information Technology

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer
security@nebraska.edu

Change Control

ITS-02

POLICY CONTENTS

Scope
Policy Statement
Reason for Policy
History

Scope

This Change Control Policy applies to all University of Nebraska Central Administration networks, systems, and services. This policy will not apply to changes made to non-production or development/test systems.

Policy Statement

A. Information Custodian/System Administrator

The information custodian/system administrator has the following responsibilities:

1. Protecting the hardware and software from unauthorized changes;
2. Assessing the risk of implementing a change;
    a. The risk assessment should include the risk of impacting the confidentiality, integrity, or availability of the systems.
3. Following a change control process, which includes the following:
    a. Establishing a process for change requests
        i. Approval of the changes with the system administrator/owner's immediate supervisor.
        ii. Coordinating the changes with other departments or campuses that might be impacted and with ITS.
        iii. Comprehensive testing of the changes in sandbox or development environments.
        iv. Identification and documentation of a back out process to execute if the change fails.
    b. Completion of a Change Request Form
    c. Approval of the Change Request by the Change Advisory Board
    d. Notification to all identified change contacts on each campus

e. Implementation and scheduling of the change with proper notification to users and management
f. Documentation of the change (to be maintained by the information custodian/system administrator)
g. Final report (log the change)

B. Emergency Changes

The change control process will accommodate the need for emergency changes.

1. Emergency change requests will require approval of a unit director in addition to the immediate supervisor.
2. The normal change management request process will be followed by completing a system change requests documenting the need for an emergency change.
3. Emergency changes will be communicated internally within all units of Central Administration.
4. Emergency changes will be communicated externally to the appropriate change management contacts within the University system.

Reason for Policy

Change control is a necessary element of stability, reliability, and quality assurance in complex technology environments. All changes to information systems (hardware and software) and networking components or architecture should follow a change management process. These changes include developing, testing, deploying, and maintaining systems and services, as well as all forms of change that may impact the physical location, configuration, and administration of assets associated with the computing and networking environments. This policy does not extend to management of personal desktops or personal file space.

History

September 19, 2017	Approved by the President
March 27, 2019	Format edited for conformance with Executive Memorandum No. 32