University of Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: *April 17, 2017*
Last Revised: *April 17, 2017*

Responsible University Administrator:
Vice President of Information Technology

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer

Change Control
IT-02

POLICY CONTENTS

Scope
Reason for Policy
Policy Statement
History

I. Scope

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

II. 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.

III. Policy Statement

A. INFORMATION CUSTODIAN/SYSTEM ADMINISTRATOR

The system owner or 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 within NU OneIT and with other departments or campuses that might be impacted.
        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 at 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 system owner or 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 request documenting the need for an emergency change.
3. Emergency changes will be communicated internally to the appropriate OneIT management and support teams.
4. Emergency changes will be communicated externally to the appropriate change management contacts within the University System.

IV. History

Approved by the President on 04/17/2017.