Information Services Change Management

POLICY CONTENTS
Scope
Policy Statement
Reason for Policy
Definitions
Related Information
History

Scope
This policy applies to any university employee, contractor, or third party who has access to university information.

Policy Statement

Change Management
To minimize the risk of data loss or corruption to university information systems, appropriate change management controls must be applied during the implementation of all information system development and maintenance activity. All production-level changes are to take place in a scheduled change window, unless proper authorization from management has deemed a change necessary or acceptable to be performed outside of the controlled change window.

Change Documentation
Documentation of changes is intended to identify and correlate a change record to a change action that is scheduled, occurring, and/or completed in the development, test, and/or production environments. All documentation of changes is to be completed in accordance with the requirements and processes identified in departmental change management procedures.

In addition, all change records are to maintain an audit trail to identify modifications to an associated change record and the party responsible for the modification. This practice ensures that the change management process is followed according to policy and procedure and that a consistent record of changes is available for review.
Change Testing
Changes must be tested prior to being implemented and regression testing must be performed post implementation. The level of required testing is determined based on the business risks associated with the information system being changed. In addition to validating that planned changes to information systems are working properly, system acceptance testing must include regression testing of other system functions to ensure that the new changes have not corrupted other system processes or data.

Change Approval
Approval and review of changes is conducted regularly by the Change Advisory Board (CAB) and as needed by the Chief Information Officer (CIO) for emergency changes as documented in departmental change management procedures.

Change Notification
Notification of documented changes are sent via email to the affected parties. In addition, change management meetings are held as outlined in the UNO Information Services Change Advisory Board Charter.

Reason for Policy
In order to protect the confidentiality, integrity, and availability of production data, this policy is meant to ensure standardized methods and procedures are used for efficient and prompt handling of all changes associated with the university’s IT infrastructure and business services.

This policy affects all identified PCI systems along with campus-wide implemented systems. Those systems that are not centrally managed are to use this policy as a best practice for change management within their respective information system environments.

Definitions

Information System: All systems that are owned, operated, or contracted by the university.

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26
UNO Privacy Policy
UNO Digital Security Incident Response Policy

This policy covers the following sections of ISO 27001:

- 10.1.2 Change management
- 12.4.1 Control of operational software
- 12.5.1 Change control procedures
• 12.5.2 Technical review of applications after operating system changes
• 12.5.3 Restrictions on changes to software packages

This policy covers the following sections of PCI-DSS 3.2:

• 6.4 Follow change control processes and procedures for all changes to system components.

History

This policy is an update to the Information Services Change Management Policy that was previously updated in 2015.