UN Change Management PCI Policy

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 PCI DSS information.

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

Change Management

To minimize the risk of data loss or corruption to university information systems transmitting or redirecting transmission of PCI DSS information, 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 the change management process is followed according to policy and procedure and 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 PCI DSS related information system being changed. In addition to validating planned changes to information systems are working properly, system acceptance testing must include regression testing of other system functions to ensure the new changes have not corrupted other system processes or data.

Change Approval

Approval and review of changes is conducted regularly by a 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 necessary.

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 PCI DSS related IT infrastructure and business services.

Definitions

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

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26

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 a new policy created in 2017.