UN Data Retention and Disposal PCI Policy

POLICY CONTENTS

Scope

This policy applies to all university personnel and entities that have access to PCI DSS cardholder data.

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

Retention

It is the policy of the university and its affiliated entities to ensure the privacy and security of proprietary and regulated information in the maintenance, retention, and eventual destruction/disposal of such media. All destruction/disposal of media storing cardholder data will be performed in accordance with federal and state law and pursuant to the university Record Retention Schedule. Records that have satisfied the period of retention will be destroyed or disposed in an appropriate manner.

The retention schedule for destruction or disposal shall be suspended for records involved in any open investigation, audit, or litigation. Individuals who know or suspect confidentiality has been breached by another person or persons have a responsibility to report the breach to the respective supervisor or administrator or to the Human Resources Department. Employees must not confront the individual under suspicion or initiate investigations on their own since such actions could compromise any ensuing investigation. All individuals are to cooperate fully with those performing an investigation pursuant to this policy.

Disposal/Destruction

Department administration shall determine what information entrusted to their department is private and/or confidential (regulated) and shall communicate methods of protecting that information through the destruction/disposal process to appropriate persons associated with their department.

All paper waste that may contain cardholder data must be shredded in compliance with regulations surrounding that material. Departments are responsible for properly disposing of the recycled material in a secure manner and ensuring all documentation necessary for demonstrating compliance with regulations is maintained within the department or by another university department tasked with this responsibility. Failure to appropriately dispose or destroy cardholder information may result in sanctions, or, suspension or revocation of accepting payment cards.

All electronic media that contains PCI DSS data must be sanitized prior to disposal.

Reason for Policy

Retention and subsequent destruction/disposal of PCI DSS data is governed by the PCI Security Standards Council, and university policies and procedures. These regulations and guidelines include, but may not be limited to:

- NU Record Retention Schedule
- PCI DSS

Definitions

PCI DSS or Cardholder Data: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26
State of Nebraska Consumer Notification of Data Security Breach Act of 2006
NU Record Retention Schedule

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

- 9.7 Maintain strict control over the storage and accessibility of media.
- 9.8 Destroy media when it is no longer needed for business or legal reasons.

History

This policy is a new policy created in 2017.