UNIVERSITY OF NEBRASKA AT OMAHA

Effective: 01-31-2015
Last Revised: 08-01-2016

Responsible University Administrator:
Chief Information Officer

Responsible University Office:
Information Security

Policy Contact:
Information Security • security@unomaha.edu

Primary Account Number (PAN) Data Security

POLICY CONTENTS

Scope
Policy Statement
Reason for Policy
Procedures
Definitions
Additional Contacts
Related Information
History

Scope

This policy applies to all university personnel and entities responsible for managing and supporting systems within the scope of PCI, as well as those responsible for the acceptance and processing of payment card transactions.

This policy affects those PCI identified systems along with campus-wide implemented systems. Systems that are not centrally managed are to use this policy as best practice for information systems security within their respective information systems environments.

Policy Statement

The University of Nebraska Omaha (UNO) will ensure that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies and that they adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI-DSS) initiatives.

Primary Account Numbers (PAN) will not be sent unencrypted via the following:

- Email
- Instant Messaging
- Chat forums
- Other applicable end-user technology

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols such as AES-128 encryption and the TLS 1.2 network protocol.

Reason for Policy

In accordance with PCI-DSS requirements, UNO has established a formal policy supporting procedures regarding the encryption of PAN that are sent via electronic transmission.

Procedures

The procedures, which ensure that the unencrypted Primary Account Numbers (PAN) policy adheres to the requirements set forth for PCI-DSS compliance require observance of the aforementioned policies.

Definitions

Primary Account Number (PAN): Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

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.

Encryption: Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

Related Information

UNO Systems Access Control Policy

UNO Retention and Destruction/Disposal of Regulated Information Policy

---

References

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

- 3.4 Render PAN unreadable anywhere it is stored

History

This policy is an update to the Primary Account Number (PAN) Data Security Policy that was previously updated in 2015.