UN Primary Account Number (PAN) Data Security PCI Policy

POLICY CONTENTS

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 all university PCI identified systems, regardless if centrally managed.

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

The University of Nebraska will ensure unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies and 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
- Fax
- 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.

Cardholder data will not be processed, transmitted, or stored on the university network.

Reason for Policy

In accordance with PCI-DSS requirements, the university has established a formal policy regarding the encryption of a PAN sent via electronic transmission.

To limit the scope of the cardholder data environment, cardholder data will not be processed, transmitted, or stored on the university network.

Definitions

Primary Account Number (PAN): Acronym for primary account number and 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.

University Network: Technology used to store or transmit data.

Related Information

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

- 3.4 Render PAN unreadable anywhere it is stored
- 3.6 Document and implement key management processes
- 4.2 Never send unprotected PANs by end-user message technologies

History

This policy is a new policy created in 2017.

The University of Nebraska shall not discriminate based upon age, race, ethnicity, color, national origin, gender-identity, sex, pregnancy, disability, sexual orientation, genetic information, veteran's status, marital status, religion, or political affiliation.