UNIVERSITY OF SOUTH DAKOTA

Policy Number:	2.040
Originating Office:	Financial Affairs
Responsible Executive:	Vice President of Financial Affairs
Date Issued:	09/07/2012
Date Last Revised:	09/07/2012

Primary Account Number (PAN) Encryption

Policy Contents

I. REASON FOR THIS POLICY

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, the University of South Dakota (USD) has established a formal policy and supporting procedures regarding unencrypted Primary Account Numbers (PAN) that are not to be sent via end-user messaging technologies. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding USD's needs and goals. This policy is to be implemented immediately and the provisions below set forth the framework regarding unencrypted Primary Account Numbers (PAN), which, again, are not to be sent via end-user messaging technologies.

II. STATEMENT OF POLICY

USD 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 (Security Standards Council 2009):

- Primary Account Numbers (PAN) will not be sent via
  - unencrypted e-mail
  - an instant messaging protocol
  - a chat protocol or forum sessions

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). Only trusted keys and/or certificates can be accepted. For SSL/TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment.

III. 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.

IV. PROCEDURES

The procedures, which ensure that the unencrypted Primary Account Numbers (PAN) policy adheres to the requirements as set forth for Payment Card Industry Data Security Standards (PCI DSS) compliance, require observance of the aforementioned policies.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Card Holder Data Access Control Policy

Card Holder Data Retention Policy

Disposing of and Destroying Card Holder Data

Management of Service Providers Policy

PCI Employee Facing Technology Policy

PCI Security Policy