UNIVERSITY OF SOUTH DAKOTA

Policy Number:	2.037
Originating Office:	Financial Affairs
Responsible Executive:	Vice President of Financial Affairs
Date Issued:	09/07/2012
Date Last Revised:	09/07/2012

Card Holder Data Retention

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 data retention and disposal. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding USD's needs and goals.

SAQ_C Requirement 3

II. STATEMENT OF POLICY

Cardholder data will be retained in accordance with Payment Card Industry Data Security Standards (PCI DSS) provisions, which allow for certain data elements to be stored while other data elements are not. The display of the Primary Account Number (PAN) information will be masked, however limited employees and other parties with a legitimate need may view the entire PAN information if necessary. The following tables list the maximum period of time cardholder data elements can be stored based on storage medium.

Electronic Media Storage of Cardholder Data

Type of Cardholder Data	Retention Period	Business Justification/Requirements for Retention of Cardholder Data
Primary Account Number (PAN)	5 minutes	Can only be stored while waiting for an authorization
Cardholder Name	5 minutes	Can only be stored while waiting for an authorization. If not stored along with the PAN, the cardholder name can be kept for 1 year.
Expiration Date	5 minutes	Can only be stored while waiting for an authorization
Service Code	5 minutes	Can only be stored while waiting for an authorization
Full Magnetic Strip/Track Data (Track 1 and Track 2)	Cannot be stored	
Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes	Cannot be stored	
Pin and Pin Block	Cannot be stored	

Hard Copy Format Storage of Cardholder Data

Type of Cardholder Data	Retention Period	Business Justification/Requirements for Retention of Cardholder Data
Primary Account Number (PAN)	1 week	All printed receipts should only contain the truncated PAN. Paper copies of forms that contain the PAN information may be kept for a period of one week to allow time to enter the transaction.
Cardholder Name	1 week	Cardholder name can only be stored with the PAN for a period of one week to allow time to enter the transaction.
Expiration Date	1 week	Expiration date can only be stored for a period of one

		week to allow time to enter the transaction.
Service Code	1 week	Service code can only be stored for a period of one week to allow time to enter the transaction.
Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes	Cannot be stored	
Pin and Pin Block	Cannot be stored	

Once the maximum retention period has been allotted for cardholder data it must be securely removed from all electronic media, and any hardcopy edition must be disposed of according to SDBOR procedures.

III. DEFINITIONS

Card Verification Code or Value: Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CVC, CVV or CSC, depending on payment card)

CVC – Card Validation Code (MasterCard payment cards)
CVV – Card Verification Value (Visa and Discover payment cards)
CSC – Card Security Code (American Express)

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.

Service Code: Three-digit or four-digit value in magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such

as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.

Personally Identifiable Information: Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.
PIN: Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.

PIN Block: A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.

IV. PROCEDURES

Any software that processes credit card information via Web must be approved and reviewed by the USD PCI officer and the USD ITS department to verify acceptable business justification for processing authorization.

POS terminal receipts must be programmed to mask the PAN information. A properly masked number will show only the first six and the last four digits of the PAN. Contact the Business Office if PAN receipt information is not truncated.

Hardcopies containing any PAN information must be shredded in a timely manner according to the USD Destroying Card Holder Data Policy.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Card Holder Data Access Control Policy

Disposing of and Destroying Card Holder Data

Management of Service Providers Policy

PAN Encryption Policy

PCI Security Policy