



Policy Number:	2.038
Originating Office:	Financial Affairs
Responsible Executive:	Vice President of Financial Affairs
Date Issued:	12/19/2014
Date Last Revised:	12/19/2014

Cardholder Data Retention, Disposing of and Destroying Cardholder Data

Policy Contents

I. Reason for this Policy.....	1
II. Statement of Policy	1
III. Definitions.....	3
IV. Procedures	4
V. Related Documents, Forms and Tools.....	4

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, disposal of and destroying cardholder data. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding USD’s needs and goals.

Reviewed by PCI Group 12/2014

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 PAN information will be masked, however limited employees and other parties with a legitimate need may view the entire PAN information if necessary.

Electronic Media Storage of Cardholder Data

Type of Cardholder Data	Business Justification/Requirements for Retention of Cardholder Data
<ul style="list-style-type: none"> • Primary Account Number (PAN) • Expiration Date • Service Code 	Can only be stored while waiting for an authorization
<ul style="list-style-type: none"> • Cardholder Name 	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.
<ul style="list-style-type: none"> • Full Magnetic Strip/Track Data (Track 1 and Track 2) • Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes • Pin and Pin Block 	Cannot be stored

Hard Copy Format Storage of Cardholder Data

Type of Cardholder Data	Business Justification/Requirements for Retention of Cardholder Data
<ul style="list-style-type: none"> • Primary Account Number (PAN) • Expiration Date • Service Code 	Paper copies of forms that contain the PAN, cardholder name, expiration date or service code may be kept for a period of one week to allow time to enter the transaction. The information must be secured at all times and destroyed after processed.
<ul style="list-style-type: none"> • Cardholder Name 	Printed receipts should only contain the truncated PAN and cardholder name. The receipts must be securely stored and destroyed one year after the close of the fiscal year.
<ul style="list-style-type: none"> • Card Verification Code or Value CID, CAV2, CVC2, CVV2 Codes • Pin and Pin Block 	Cannot be stored

Once the maximum retention period has been allotted for cardholder data it must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly. Methods for disposal including the following:

- Purging and deleting cardholder data from all system components. This can be done by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion (i.e., degaussing). System components are defined as any network component, server or application included in or connected to the cardholder data environment.
- Destroying (cross-shredding) any cardholder data that is in a hardcopy format.

For electronic media stored on system components that are no longer in use, these system components must have cardholder data disposed of via any one of the following procedures:

- Disintegration
- Shredding (disk grinding device)
- Incineration by a licensed incinerator
- Pulverization

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.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Credit Card Acceptance 2.041

<http://www.usd.edu/policies/business-and-administration.cfm>

Management of Service Providers 2.039

<http://www.usd.edu/policies/business-and-administration.cfm>