Retention and Disposal

Payment Card Industry (PCI) Data Security Standard (DSS) requirement 3.1 requires that the university maintain and adhere to a data retention and disposal procedures. The purpose of this procedure is to ensure that records that are no longer needed are discarded appropriately and in a timely fashion. Each area that takes credit cards as payment must periodically (annually) review these procedures to determine if any circumstances that necessitate changes in the way they retain or dispose of cardholder data.

Emory University/Emory Healthcare is required to be compliant with the PCI-DSS. Non-compliance can result in fines to merchants of at least $10,000 per month and $500,000 per card brand (American Express, Visa, MasterCard) if there is a data breach.

PCI DSS applies whenever account data is stored, processed, or transmitted. Account Data consists of Cardholder Data plus Sensitive Authentication Data, as follows:

Cardholder Data Includes:	**Sensitive Authentication Data Includes:**
Primary Account Number (PAN)	Full magnetic stripe data or equivalent on a chip
Cardholder Name	CAV2 / CVC2 / CVV2 / CID
Expiration Date	PINs / PIN blocks
Service Code	

1.1 Storage

- The following credit card information is permitted to be stored only if there is an approved and documented business need. All data must be protected as described in all sections of the PCI DSS. The following card holder data, protected as required by the PCI DSS and approved by the Office of Treasury/Debt Management, is permitted to be stored under this provision:

Type of Cardholder Data	**Retention Period**
➢ Primary Account Number (PAN)	Can only be stored while waiting for an authorization*
➢ Cardholder name	Can only be stored while waiting for an authorization*
➢ Service Code	Can only be stored while waiting for an authorization*
➢ Expiration Date	Can only be stored while waiting for an authorization*

** If not stored along with the PAN, this data element can be retained for up to 2 years*

The following card holder data is not permitted to be stored:

➢ Full Magnetic Stripe (Track 1 or 2 data)	Cannot be stored
➢ CVV2, CVC2, CID, CAV2	Cannot be stored
➢ PIN / PIN Block	Cannot be stored

- Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction.
- System and audit logs showing access to stored data must be retained for at least 1-year. Logs must be kept online and available for 90 days.

1.2 Disposal

- All sensitive and credit card data must be destroyed when it is no longer required by legal, contractual, or business need.
- Techniques for disposal of data on media is as follows:
  - Hard disks: must be overwritten as prescribed by the Emory University Electronic Data Disposal Policy or physically destroyed.
  - Floppy disks: must be shredded.
  - Optical media (CD's, DVD's, Blue Ray, etc.) must be shredded
  - Other magnetic media, (USB Drives, storage cards, etc.) must be overwritten by an approved method, or as prescribed by the
  - Paper: must be cross-cut shredded, pulped or incinerated Emory University Electronic Data Disposal Policy or otherwise destroyed.
  - Paper containing cardholder data, awaiting destruction, must be stored in a secure containers secured with a lock to prevent access to its contents.
  - Quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements must be in place.

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 Card Holder Data Retention 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.