Data Retention and Disposal Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures concerning data retention and disposal. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will ensure that the Data Retention and Disposal policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Comprehensive policies, procedures, and processes are to be developed, implemented, and in place regarding the following:
    - All legal, regulatory, and business requirements for data retention. Specifically, limiting data storage amount and retention time to that which is required for the applicable legal, regulatory, and business requirements.
    - Specific requirements for retention of cardholder data, such as why cardholder data needs to be held (i.e., time period) and the reasons why (i.e., business justification).
    - Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons.
    - Coverage for all storage of cardholder data.
    - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.
    - Additionally, all locations of stored cardholder data are to be included in the data retention and disposal processes.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the data stored does not exceed the requirements defined in the data retention policy.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that data is deleted securely.

Description of Data and Scope for Cardholder Environment

Cardholder data, as defined by the Payment Card Industry Security Standards Council (PCI SSC) Glossary of Terms, includes, at a minimum the Primary Account Number (PAN), and may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or the service code. Additionally, cardholder data may also include Sensitive Authentication Data, such as security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, which appears in plain-text or otherwise unprotected form. This cardholder data may reside in numerous places throughout the cardholder environment.

DESCRIPTION OF KEY TERMS AND PHRASES

- **Access Control:** Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.
- **Cardholder Data:** The Primary Account Number (PAN) may also appear in the form of the full PAN, plus any of the following:
    - Cardholder name
    - Expiration date
    - Service code
- **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).

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

- **Data:** Pieces of information from which *intelligible information* is derived. Data is a collection of information or facts usually gathered as the result of experience, observation, experiment or processes within a computer system or premises. Data may consist of numbers, words or images, particularly as measurements or observations of a set of variables. They are often viewed as the lowest level of abstraction from which information and knowledge are derived.

- **Database:** Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.

- **Degaussing:** Also called disk degaussing, it is the process or technique that demagnetizes the disk so that all data stored on the disk are permanently destroyed.

- **Encryption:** Process of converting information into a form only intelligible to holders of a specific cryptographic key. The use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

- **Full Magnetic Stripe Data:** Also referred to as *track data*. Data encoded in the magnetic stripe or chip is used for authorization during payment transactions. It can be the magnetic stripe image on a chip or the data on the Track 1 and/or Track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.

- **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.

- **Removable Electronic Media:** Media that store digitized data and can be easily removed and/or transported from one computer system to another. Examples of

removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.

- **Hardcopy Media:** Hardcopy media are physical representations of information stored. Examples of hardcopy media include, but aren't limited to: paper printouts or other documents, credit card or other paper receipts, invoices, purchase orders, and batch printouts.
- **Sanitization:** Process for deleting sensitive data from a file, device or system or for rendering data useless if accessed in an attack.
- **Secure Wipe:** Also called *secure delete*, this is a program utility used to delete specific files permanently from a computer system.
- **Sensitive Authentication Data:** Security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.
- **Service Code:** Three- 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.
- **System Components:** Any network component, server or application included in or connected to the cardholder data environment.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019