Version:	Modified By:	Date:	Approved By:	Date:
1.0	Lisa Zaelit	February 7, 2014	Dan Bowden	February 28, 2014
2.0	Kim Stringham	August 12, 2015	Lisa Zaelit	August 18, 2015
3.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 3 – Protect Cardholder

Data: Purpose

The purpose of having procedures for data retention and storage is to ensure that only necessary, required data is retained and stored securely.

Procedure

A. Data Retention and Storage – Standard 3.1

1. Card holder data stored on paper:
    a. Card holder data (CHD) taken by phone for payments, should be processed immediately.
        i. Once processed, the paper containing CHD should be immediately redacted or destroyed by using a cross cut shredder.
    b. Acceptance of CHD by fax or e-mail should be discouraged, and definitely not promoted.
    c. Only the cardholder name, address, card number, and expiration date should be put on paper.
    d. All CHD stored on paper, shall be destroyed within 24 hours.
        i. The paper should be destroyed by using a cross cut shredder.
    e. Departments should report annually that there is no CHD being stored beyond the procedures stated above. Any exceptions, or the business need to hold any CHD, should be confirmed with Income Accounting and Student Loan Services, and supporting documentation should be sent to Income Accounting.
2. Cardholder data stores on electronic media:
    a. If it is necessary to store any CHD by electronic media, it should be encrypted, and on devices that are segmented behind a PCI firewall, have monthly vulnerability scans, daily logging, and potentially annual penetration testing as applicable.
    b. Devices should also be hardened, have file integrity monitoring, anti-virus, and Identity Finder.
    c. CHD shall be deleted from electronic media every 90 days.

B. **Sensitive Card Holder Data –** Standard 3.2

Procedure

1. All Department point of contacts shall sign an annual document which states they are not storing sensitive data.
    a. Departments must demonstrate a business need to retain sensitive cardholder data.
    b. Sensitive authentication data, including CVV or CVC, PIN or PIN Blocks, or full track data (from magnetic stripe or equivalent on a chip), will never be stored.

2. Identity Finder scans shall occur monthly, for any department storing CHD on electronic media.

C. **Cardholder Data Stored on Removable Media –** 3.4

1. CHD shall never be stored on removable media unencrypted.
    a. If disk encryption is not used to encrypt removable media, another method shall be used to render the data unreadable, by another method.

2. CHD shall never be stored on a spreadsheet.

3. All Department points of contact shall sign a document annually, which states they are not storing sensitive data on removable media.