CODE NO. 101.1

NOVA SOUTHEASTERN UNIVERSITY

POLICY STATEMENT

SECTION: FOP-TREASURY DEPARTMENT

SUBJECT: Payment Card Data Retention and Disposal Policy

Overview

Nova Southeastern University's (NSU) Payment Card Data Security Policy (FOP- Treasury Policy No. 101) requires that all personnel and departments that accept, process, transmit, or store payment cardholder information comply with the Payment Card Industry Data Security Standards (PCI DSS) for proper handling of credit/debit card data. This policy statement concerns retention and disposal of payment card data and is to be implemented in conjunction with Policy No. 101.

Policy

NSU shall comply with Section 3.1 of PCI DSS by keeping cardholder data storage to a minimum. Extended storage of cardholder data that exceeds business need creates an unnecessary risk. Accordingly, all personnel and departments that store payment cardholder information shall:

- Limit data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Maintain a process for secure deletion of data when no longer needed
- Execute specific retention requirements for cardholder data
- Conduct a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements

The only cardholder data that may be stored after authorization is the primary account number (PAN), rendered unreadable, and the expiration date, cardholder name, and service code.

Application

Procedures for data retention and disposal must be maintained by each department that stores cardholder information and must include the following:

- All physical records reflecting cardholder data must be locked in a desk drawer or file cabinet when not in immediate use by staff. Access to secure areas must be limited to the appropriate individuals as recognized by the department. Furthermore, appropriate facility controls must be used to limit and monitor physical access to systems that store cardholder data.

NOVA SOUTHEASTERN UNIVERSITY

POLICY STATEMENT

SECTION: FOP-TREASURY DEPARTMENT

SUBJECT: Payment Card Data Retention and Disposal Policy

- Cardholder data should be retained for one year or less, depending on the business needs of the department. Business needs include the ability to access cardholder data for purposes of processing credits on previous payments. It is not anticipated that cardholder data would be needed beyond a one year period for legal, regulatory, or business reasons. Therefore, NSU has established a general cardholder data retention period limit of one year.

- At the end of the established retention period, media must be destroyed by the following methods so that the cardholder data cannot be reconstructed (PCI DSS Section 9.8):

    - Cross-cut shred, incinerate, or pulp hardcopy materials
    - Render cardholder data on electronic media unrecoverable by securely wiping, purging, degaussing, or physically destroying (such as grinding or shredding hard disks)
    - Secure storage containers used for materials that are to be destroyed

- A quarterly review must be conducted to verify that stored cardholder data does not exceed retention requirements defined herein. If utilizing the Payment Gateway server TouchNet, a programmatic (automatic) process will be used to remove stored cardholder data that exceeds the retention limit defined herein.

- No cardholder information may be entered, collected, or retained in electronic form, including spreadsheets, databases, word processing documents, flash drives, cd's, in email, or any other electronic files for the intent of data retention.