HOFSTRA UNIVERSITY
Policy and Procedures

Subject: **Credit Card Data Security Policy**
Date Last Revised: May 14, 2009
Responsible Office: Financial Affairs

Purpose

The Payment Card Industry (including VISA, Master Card, American Express, Discover, and other major card issuers) has established important and stringent security requirements to protect credit card data. The University is required to comply with these standards, which are known as the Payment Card Industry - Data Security Standards (PCI-DSS). A PCI Compliance Committee that includes representatives from Treasury, Internal Audit, and Information Technology Security has been established to monitor University compliance with PCI-DSS and advise departments on measures to achieve compliance with these standards.

Policy

All efforts must be made to maintain the tightest security and procedures in areas that process credit and debit card transactions. Departments that accept credit and debit cards must comply with PCI data security standards. Each department must submit a completed PCI-DSS Self-Assessment Questionnaire that attests to their compliance with PCI-DSS standards annually to the Office of Financial Affairs.

Important aspects of credit card security include, but are not limited to, the following:

- All credit card information must be kept secure and confidential.
- The credit card 3- or 4-digit service code (CVV2 code) must never be written down, retained, or stored in any fashion.
- Only authorized employees should access and process credit card transactions.
- Non-traditional employees, such as students, temporary employees, etc., must never have unsupervised access to confidential payment card data, both electronic and paper, including areas where credit card information is processed and/or maintained.
- Sensitive cardholder data cannot be stored in any fashion on University computers or networks, unless prior review and approval has been received by the Office of Financial Affairs, and then only in a secure encrypted manner as approved by the PCI Compliance Committee.
- Credit card account numbers must never be transmitted in an unsecure manner, such as by unencrypted email or unsecured fax. Paper documents containing credit card information should be labeled confidential. Credit card numbers, except for the last four digits, should be redacted from a document whenever possible.
- Orders for new credit card swipe machines or other equipment used to process credit cards must be approved by the Office of Financial Affairs. Unused or broken credit card swipe machines must be returned to the Office of Financial Affairs.

- Refunds, partial or whole, for any transactions originally processed through a credit or debit card must be made only to the original card holder through the credit or debit card used in the original transaction. All refunds must be approved and signed off by the appropriate senior manager within the department. At a minimum, the original transaction charge, refund amount and supporting documentation (e.g., receipts, printouts, etc) must be attached to a signed (i.e., management approval) refund request form.
- Documentation containing credit card information must be maintained in a secure environment limited in access to appropriate and authorized personnel. Secure environments include locked desk drawers and locked file cabinets, located in locked offices, as well as safes.
- Documentation authorizing credit card transactions on behalf of the cardholder must be kept for a minimum of 18 months. After 18 months (longer, if the University's Document Retention Policy requires it for that particular document type), the documentation must be destroyed in a manner that will render it unreadable through the use of a cross-cut shredder or by incineration.

Third-Party Service Providers

Any department that seeks to engage a third-party company that will accept payment by credit or debit card on behalf of the University, including, but not limited to, tuition-related payments, event registrations, items for sale, or to accept donations, in-person or online, must request prior authorization from the Office of Financial Affairs. The University must only engage third-party companies that are certified as compliant with, and/or contractually state they adhere to, Payment Card Industry – Data Security Standards (PCI-DSS).

Reporting Credit Card Data Security Incidents

Departments that process credit and/or debit card payments must be vigilant and alert to potential incidents where cardholder information may have been compromised. Events that may signal credit card information has been compromised may include the following:

- suspicious behavior
- lapses in security of or unusual activity within areas where credit card data is stored
- sensitive information being found in the wrong place or hands
- unauthorized use of credit card processing equipment or software
- customer reports of problems with credit cards

Departments that believe a security breach may have occurred should contact the Office of Financial Affairs immediately. An investigation by the Office of Financial Affairs will be undertaken, with assistance from Public Safety, Internal Audit, and Information Technology Security, as required by the circumstances.