CODE NO. 101.2

NOVA SOUTHEASTERN UNIVERSITY

SECTION: FOP- TREASURY OFFICE

SUBJECT: PCI-DSS General Guidelines and Procedures

NSU NOVA SOUTHEASTERN UNIVERSITY

SECTION: FOP- TREASURY OFFICE

SUBJECT: PCI-DSS General Guidelines and Procedures

1. Introduction

1.1. Purpose and Background

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 debit or credit card data. The following general guidelines and procedures supplement Policy No. 101 and are to be implemented in conjunction with Policy No. 101.

NSU accepts credit/debit card payments as a convenience to our students/customers. Departments may accept Visa, MasterCard, American Express, and debit cards with a Visa or MasterCard logo. Individual business units or departments that process credit/debit card payments are assigned unique merchant accounts.

1.2. Central Coordinator Contact

The University's Treasurer, with the assistance of the designated Coordinator of Electronic Payment Services within the Treasury Office, serves as the central "Coordinator" for payment card activity throughout the University. Approval from the Coordinator is required before a credit/debit card merchant account can be established. The Coordinator manages all applications to create merchant accounts or to make changes to an existing account. Contact the Coordinator at treasury@nova.edu, or:

Treasury Office - Coordinator of Electronic Payment Services
Ava Davis R-510 (East Campus)
3301 College Avenue
Fort Lauderdale, FL 33314
Phone: (954) 262-5298
ava@nova.edu

1.3. PCI Data Security Standards - High Level Overview

A link to the PCI-DSS is included in the final section of this document. There are twelve main requirements summarized as follows:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Identify and authenticate access to system components
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for all personnel

2. PCI-DSS Guidelines – Division of Responsibilities

This section includes a summary of the main requirements from PCI-DSS for which each subgroup below is responsible. It is not, however, intended to be a complete list of all PCI-DSS requirements. As indicated in Policy No. 101, compliance with all PCI-DSS is required.

2.1. Requirements Applicable to All Personnel with Access to Payment Card Information

The PCI-DSS always applies where primary account numbers (PANs) are stored, processed, or transmitted. All personnel with access to payment card information:

A. May not sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party. All requests to provide information to any party outside of your department must be coordinated with the Coordinator in the Treasury Office. This applies also to contractors or agents who obtain access to payment card or other personal payment information in the course of conducting business on behalf of NSU.

B. Will be subject to background screening prior to hire to minimize the risk of attacks from internal sources. Refer to the Employee Policy Manual maintained by the Office of Human Resources. **PCI 12.7.**

Annually:

C. Sign the Payment Card Data Security Policy Acknowledgement & Training Certification form (available on the Treasury Office website or via SharkTalent certification upon completion of online training) to: 1) document his/her understanding of and willingness to comply with all university payment card security policies, directives and procedures and PCI-DSS, and 2) confirm required training has been completed as described below. This certification will be maintained in the merchant's file with the Treasury Office and should be submitted to the Coordinator during establishment of a new merchant location, the hiring of a new employee, and on an annual basis thereafter. The merchant also keeps a copy of this document on file. Temporary and student personnel shall complete the manual form, whereas all other personnel shall complete the certification electronically via SharkTalent. **PCI 12.6.**

D. Must attend a credit card information security training session upon hire and at least annually, pursuant to NSU's Security Awareness Program as indicated herein. **PCI 12.6.1, 12.6.2**

2.2. Requirements Applicable to Merchant/NSU Department Locations

A. Protect Stored Cardholder Data. PCI 3.2, 3.3, 3.4

- Prohibit the storing of the card verification code or value, or PIN. Never store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. **PCI 3.2.2**
- Do not store the personal identification number (PIN). **PCI 3.2.3**
- May not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). In the normal course of business, the following data elements from the magnetic stripe may need to be retained: **PCI 3.2.1**
    - The cardholder's name,
    - Primary account number (PAN),
    - Expiration date, and
    - Service code.

- Mask retained primary account numbers when displayed. The first six and last four digits are the maximum number of digits to be displayed. **PCI 3.3**
- Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs). **PCI 3.4**

B. Prohibit transmitting payment card information by email or fax. Never send unprotected PANs by end- user messaging technologies (for example, e-mail, instant messaging, SMS, and chat, etc.). **PCI 4.2.**

C. Limit access to system components and cardholder data to only those individuals whose job requires such access. Access controls shall incorporate the following: **PCI 7.1.**

- Define access needs and privilege assignments for each role;
- Access restrictions on privileged user IDs grant the least privileges necessary to perform job responsibilities;
- Access assignments are based on individual personnel's job classification and function;
- Approval documentation (electronically or in writing) is administered by authorized parties for all access, including listing of specific privileges approved.

D. Ensure restricted access based on a business need to know. **PCI 7.2**

E. Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. Develop procedures to easily distinguish between onsite personnel and visitors in areas where cardholder data is accessible; procedures to include the proper handling of visitors including use of a log, as described in the PCI-DSS. **PCI 9.1 - 9.4.**

F. Physically secure all media and verify the storage location is reviewed at least annually. **PCI 9.5, 9.5.1**

G. Classify the media so it can be identified as confidential. PCI 9.6.1.

H. Protect devices that capture payment card data vis direct physical interaction with the card from tampering and/or substitution. PCI 9.9.

I. Inspect card-reading devices monthly to look for tampering and/or substitution. **PCI 9.9**

J. Submit evidence of periodic inspections on card-reading devices to the Coordinator.

K. Maintain an up-to-date list of card reading devices that include **PCI 9.9**:
   a. Make, model of devices;
   b. Location of devices (address);
   c. Device serial number or other method of unique identification.

L. Retain and dispose of media containing cardholder data in accordance with the Payment Card Data and Retention Disposal Policy (FOP- Treasury Policy No. 101.1).

M. Be prepared to follow security incident response and escalation procedures to ensure timely and effective handling of all situations. . Refer to the Incident Response Plan in the NSU Office of Innovation and Information Technologies policy and procedure manual.

N. Segregate duties. Establish appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.

Quarterly:

O. Ensure a programmatic (automatic or manual) process to remove, at least on a quarterly basis, stored cardholder data that exceeds requirements defined in the data retention policy. Refer to Payment Card Data and Retention Disposal Policy (FOP- Treasury Policy No. 101.1).

Annually:

P. Verify that the storage location is reviewed at least annually to determine that back-up media storage is secure. **PCI 9.5.1** Properly maintain inventory logs of all hardcopy media and conduct inventories at least annually. **PCI 9.9.1.**

Q. Perform an annual self-assessment and report the results to the Coordinator. The PCI-DSS Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI-DSS. Management in departments accepting payment cards must conduct the annual self-assessment and report the results to the Coordinator. The Coordinator will notify each department head of the timeline to complete and submit the annual assessment. The annual assessment must be completed by the merchant account owner annually and anytime a payment card related system or process changes.

R. Ensure all departmental personnel with access to payment card information have completed the following:

- Signed the Payment Card Data Security Policy Acknowledgement & Training Certification form (available on the Treasury Office website or via SharkTalent certification upon completion of online training) to: 1) document his/her understanding of and willingness to comply with all university payment card security policies, directives and procedures and PCI-DSS, and 2) confirm required training has been completed as described below. This certification will be maintained in the merchant's file with the Treasury Office and should be submitted to the Coordinator during establishment of a new merchant location, the hiring of a new employee, and on an annual basis thereafter. The merchant also keeps a copy of this document on file. Temporary and student personnel shall complete the manual form, whereas all other personnel shall complete the certification electronically via SharkTalent. PCI 12.6.
- Must attend a credit card information security training session upon hire and at least annually,pursuant to NSU's Security Awareness Program as described herein. **PCI 12.6.1, 12.6.2**

2.3. Requirements Applicable to the Treasury Office (the Coordinator)

A. Establish, publish, maintain and disseminate a security policy that addresses all PCI-DSS requirements. **PCI 12.1.** Refer to Payment Card Data Security Policy (FOP- Treasury Policy No. 101).

B. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes. **PCI 3.1.** Refer to Payment Card Data and Retention Disposal Policy (FOP- Treasury Policy No. 101.1).

C. Manage Service Providers. **PCI 12.8.**
- Maintain a comprehensive list of service providers. **PCI 12.8.1**
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. **PCI 12.8.2**
- Monitor service providers' PCI-DSS compliance status annually. The review will include reconfirmation of certified PCI compliance of NSU's third party vendors that accept payment card payments on behalf of the University. **PCI 12.8.4**

D. Maintain the Security Awareness Program (see section 3.5 below). **PCI 12.6.**

Annually:

E. Review the security policy at least annually and update as needed to reflect changes to business objectives or the risk environment. **PCI 12.1.** Refer to Payment Card Data Security Policy (FOP- Treasury Policy No. 101).

F. Perform an annual self-assessment in partnership with an independent compliance partner that is certified by the cardholder industry, if required.

G. Ensure that all departments have completed the necessary training and submitted to the Coordinator:
- The annual self-assessment
- Payment Card Data Security Policy Acknowledgement & Training Certification forms or electronic transcripts for all applicable personnel

2.4. Requirements Applicable to the Office of Innovation and Information Technologies (OIIT)

A. Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. **PCI 5.1.**

B. Develop and maintain secure systems and applications. **PCI 6**. Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. **PCI 6.2**.

C. Assign authorized users a unique ID before allowing them to access system components or cardholder data. User names and passwords may not be shared. **PCI 8.1.1 /8.5.**

D. Store electronic media back-ups in a secure location, preferably an off-site facility, such as an alternate or back- up site, or a commercial storage facility. Classify the media so it can be identified as confidential. **PCI 9.5, 9.6.1**

E. Establish firewall and router configuration standards. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e- commerce, personnel's internet access through desktop browsers, personnel's e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. **PCI 1.1, 1.1.1**

F. Review logs at least daily of all system components that store, process, or transmit card holder data and/or sensitive authentication data, of all critical system components, and of all servers and system components that perform security functions (examples include firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc). **PCI 10.6.1**

G. Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up). **PCI 10.7.**

H. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. **PCI 12.5.1** Implement an incident response plan to respond immediately to a system breach. **PCI 12.10**. Refer to the OIIT policy and procedure manual for the Information Security Incident Response Plan.

I. Processes and procedures for cryptographic keys used for encryption of cardholder data: Verify that key-management procedures are implemented to require crypto-periodic key changes. **PCI 3.6.4**

Quarterly:

J. Change user passwords at least every 90 days. **PCI 8.2.4.**

K. Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use. **PCI 11.1.**

L. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **PCI 11.2.**

Biannually:

M. Review firewall and router rule sets. - Requirement to review firewall and router rule sets at least every six months. **PCI 1.1.7**

Annually:

N. Conduct an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment. **PCI 12.2**

O. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. **PCI 6.6.**

P. In collaboration with the Internal Auditing department, perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub network added to the environment, or a web server added to the environment) **PCI 11.3.1**

Q. Verify that the storage location is reviewed at least annually to determine that back-up electronic media storage is secure. **PCI 9.5.1**

R. Properly maintain inventory logs of all electronic media and conduct media inventories at least annually. **PCI 9.7.1**

S. Test the incident response plan at least annually. **PCI 12.10.2**

3. *General Procedures*

3.1. General Guidelines When Accepting Payment Cards

The following are general guidelines for all NSU merchants:

- Approved payment card swiping machines or approved third-party software are used for processing all transactions.
- Charge cards shall be accepted for no more than the amount of purchase.
- The signature on the charge card, if available, must agree to the draft.
- The expiration date on the credit card must be verified.
- The student/customer's copy of the sales draft must include only the last four (4) digits of the credit card number. The department may retain the merchant copy and must secure these drafts against unauthorized access.
- Payment card numbers are not to be sent via e-mail or to an unsecured fax machine.
- Customer payment card numbers are not to be entered or stored on a computer unless the merchant has been approved by the Coordinator to do so.
- When customers dispute a charge, the credit card processor will communicate disputed credit card sales to the Treasury Office. Treasury will scan the information to the appropriate department for research. It is the department's responsibility to research the chargeback within the designated time period and provide all pertinent documentation to the credit card processor.
- Credit card refunds that need to be generated can be completed with a Manager's Signature and when the original sale slip is present.

3.2. Setting up Credit Card Terminal Accounts

NSU departments, who intend to process payment card transactions face-to-face or in a MO/TO (Mail Order/Telephone Order) environment, by means of a payment card swipe machine, must complete and submit the following documentation (see section **4.3.** below for accessibility of forms) to the Coordinator: treasury@nova.edu

- Request for Merchant ID (Additional Outlet Form)
- Completed Payment Card Data Security Policy Acknowledgement & Training Certification for each relevant staff member (must be completed prior to completing any payment processes)

Upon approval, the Coordinator will forward pertinent information to NSU's payment card processor who will set up the merchant, issue a merchant number, and ship a terminal to the Coordinator. The terminal will be logged in, tagged and prepared for pick up by the merchant. The merchant/NSU department will be billed directly for all equipment cost.

The fees charged by the various credit card companies are based on a variety of factors. A list of factors may be requested from the Coordinator.

The Coordinator will charge departments/merchants based on the monthly statement received from the credit card companies and the credit card processor.

3.3. Setting up a New Internet-Related E-Commerce Account

All NSU divisions, departments, and centers desiring to accept payments via the internet using E- commerce must process all sales transactions through the University web payment gateway (Touch Net). This gateway ensures that all payment card transactions meet standards specified by the PCI-DSS. To initiate new account setup, complete and submit the following documentation (see section **4.3.** below for accessibility of forms) to the Coordinator: treasury@nova.edu

- TouchNet System Account Request Form
- Completed Payment Card Data Security Policy Acknowledgement & Training Certification for each relevant staff member (must be completed prior to completing any payment processes)

3.4. Loss or Theft, Process for Responding to a Security Breach

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized individual. In the event of a breach or suspected breach of security, including the suspicion that payment card information has been exposed, stolen, or misused; the merchant/NSU departments must consult the Information Security Incident Response Plan (refer to the OIIT policy and procedure manual) and contact the appropriate individuals as set forth therein immediately.

3.5. Security Awareness Program

PCI-DSS requires a formal security awareness program to make all personnel aware of the importance of cardholder data security. **PCI 12.6** If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.
NSU's Security Awareness Program will be maintained by the Coordinator, with assistance from the Chief Information Security Officer. The Program consists of:

- All personnel with access to payment card information will be educated initially (upon hire or transfer) and at least annually.
- The method of delivery of the education will vary to suit the particular audience or training being delivered. Initial and annual training may be delivered via a formal hands-on or computer-based training session, while ongoing periodic updates will be delivered via emails, posters, newsletters, etc. It is expected that annual training will be conducted by NSU's merchant provider during the same month each year. It is also expected that the initial training will be offered via a computer-based training session in order to facilitate timely completion by new hires. However, the Coordinator may revise the delivery method of the training as appropriate.
- The focus and depth of the initial and annual training can vary depending on the role of the personnel, and may be tailored as appropriate for the particular audience.
- The Coordinator will work the Office of Human Resources, OIIT, and NSU merchants/departments to ensure all parties are aware of the training requirements under this program and that procedures are in place to facilitate and track completion.
- Upon completion of the initial and annual training, the Payment Card Data Security Policy Acknowledgement & Training Certification form will be completed by each employee. Departments must provide a copy to the Coordinator.

4. *Other*

4.1. Ongoing Policy and Procedure Management

NSU may modify existing policies and procedures from time to time as required, provided that all modifications are consistent with PCI-DSS then in effect.

The Coordinator is responsible for initiating and overseeing an annual review of the master policy statement (Policy No. 101) and related directives and procedures contained herein, making appropriate revisions and updates and disseminating the information to appropriate merchants/NSU departments.

4.2. Revision History

This document reflects relevant information as of the implementation date and subsequent revisions of Policy No. 101.

4.3. Resources- Forms and Links

A. Forms – the following are available as follows:

- Request for Merchant ID (Additional Outlet Form) (for usage of swiping machines): Contact the Coordinator at treasury@nova.edu to request form
- Payment Card Data Security Policy Acknowledgement & Training Certification: **http://www.nova.edu/treasury/forms/pci-employee-certification.pdf**
- TouchNet System Account Request Form: **http://www.nova.edu/treasury/forms/touchnet-access.pdf**
- Credit Card Machine Periodic Inspection Form **http://www.nova.edu/treasury/forms/monthly-inspection-form.pdf**
- Access Request Form for POS Systems **http://www.nova.edu/treasury/forms/access-request-form-for-pos-systems.pdf**

B. Links

- NSU OIIT policies and procedures, including PCI-DSS related matters:
  - The Acceptable Use Policy: **https://www.nova.edu/portal/oiit/policies/forms/information-security-acceptable-use-policy.pdf**
  - Information Security Policies: **http://www.nova.edu/common-lib/policies/**
- PCI Security Standards Council (contains PCI-DSS): **https://www.pcisecuritystandards.org/**
- VISA Risk Management: **http://www.visa.com/visariskproducts/downloads/bbb-visa-data-security.pdf**
- VISA "If Compromised": **https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf**