CODE NO. 101

NSU NOVA SOUTHEASTERN UNIVERSITY

POLICY STATEMENT

SECTION: FOP-TREASURY OFFICE

SUBJECT: PAYMENT CARD DATA SECURITY POLICY

Purpose

To communicate Nova Southeastern University's (NSU) policy with respect to Payment Card Industry Data Security Standards (PCI-DSS) and the requirements for proper handling of credit/debit card data.

Background

PCI-DSS are the result of the collaboration between the four major credit card brands to develop a single approach to safe guarding sensitive cardholder data. PCI-DSS defines a series of requirements for processing, transmitting and storing sensitive payment card data.

PCI-DSS applies wherever account data is stored, processed, or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, summarized as follows. The table also illustrates whether storage of the data is permitted or prohibited and whether each data element must be protected:

		Data Element	Storage Permitted	Render Stored Account Data Unreadable
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data*	Full Magnetic Stripe Data**	No	Cannot store
		CAV2/CVC2/CVV2/CID	No	Cannot store
		PIN/PIN Block	No	Cannot store

*Sensitive authentication data must not be stored after authorization (even if encrypted).

**Full track data from magnetic stripe, equivalent data on the chip, or elsewhere.

Source: Navigating PCI-DSS: Understanding the Intent of the Requirements, v3.2, January 2017; PCI Security Standards Council LLC.

NSU NOVA SOUTHEASTERN UNIVERSITY

POLICY STATEMENT

SECTION: FOP-TREASURY OFFICE

SUBJECT: PAYMENT CARD DATA SECURITY POLICY

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.

Credit/debit card merchants at NSU are required by this policy to follow strict procedures to protect student/customer payment card data as PCI-DSS compliance is required of all merchants. Accordingly, controls must be in place for handling and restricting of payment card information, computer and internet security, as well as the reporting of payment card information breaches.

Although the primary focus of the PCI-DSS is on web-based sales and processing payment card information via the internet, other services have the potential to expose cardholder information. Therefore, all NSU credit card merchants, including merchants transmitting via a terminal on a dedicated phone or Ethernet line, must comply.

Scope

This policy is applicable to all NSU departments/locations that process, transmit, or store cardholder information in a physical or electronic format. This pertains to ALL transactions, including those initiated via the telephone, over the counter, via mail order, via the internet, via fax, etc. All computers and electronic devices are governed by PCI-DSS. This includes, but is not limited to, servers that store payment card numbers, workstations that are used to enter payment card information into a central system, and any computers or credit/debit card swipe devices through which payment card information is transmitted. Furthermore, this policy applies to all personnel with access to payment card information, including employees, consultants and temporary workers, as well as any third party vendors that may process payment cards on behalf of NSU.

Policy Statements

All NSU departments/locations that accept credit/debit cards for payment of goods and services must implement adequate procedures to ensure that cardholder data is stored, transmitted and processed in compliance with PCI-DSS at all times. Specifically:

- Compliance with PCI-DSS is required of all NSU personnel and departments that accept, process, transmit, or store payment cardholder information. This includes any NSU employee, student, contractor or agent who, in the course of doing business on behalf of NSU, is involved in the acceptance of payment card and e-commerce payments for NSU.

- Only PCI-DSS compliant equipment, systems, and methods (as approved by the Coordinator defined herein) may be utilized to process, transmit, and/or store cardholder information.
- All NSU personnel who accept and/or access cardholder information, devices, or systems which store or access cardholder information:
    - must be properly trained (initial training will be supplemented through an ongoing training program),
    - must sign a statement that they have read, understand, and agree to adhere to this policy, and
    - are responsible for protecting cardholder information in accordance with PCI-DSS and NSU policy (and therefore may not acquire or disclose cardholder data, nor use said data for any unauthorized or improper purpose).
- Vendors and service providers involved in payment card transactions on behalf of NSU must contractually agree to comply with PCI-DSS, and must provide evidence of compliance annually to NSU.
- Any suspected security breach must be immediately reported and handled in accordance with NSU's Office of Innovation and Information Technologies (OIIT)'s incident response policy.

Central Coordinator Appointment

The Treasurer will serve as the Coordinator of this policy, with assistance from OIIT's Chief Information Security Officer.

The Coordinator must approve each merchant bank or processing contact of any third-party vendor involved in processing or storing payment card data on behalf of NSU. Third-party vendors include processors, software providers, payment gateways, or other service providers.

All NSU credit card merchants must prove compliance to the Coordinator by completing an annual PCI-DSS self-assessment questionnaire and, if applicable, allow for remote external scans by our PCI approved quality assessor.

All contracts or purchases of software and or/equipment related to payment card processing will be originated/approved by the Coordinator and the Chief Information Security Officer. This applies regardless of the transaction method or technology used.

Enforcement

Security breaches or lack of adherence to the requirements surrounding proper handling of credit/debit card information could result in serious consequences for NSU.

Failure to comply with the terms of these polices may result in disciplinary action up to and including termination and the possibility of civil and/or criminal liability. Additionally, an employee's violation may also result in the loss of a department's credit card acceptance privileges.

Related Policies, Procedures and Resources

The following related policies, procedures and resources provide guidance to facilitate compliance with PCI-DSS.

- Payment Card Data Retention and Disposal Policy (FOP- Treasury No. 101.1)
- PCI-DSS General Guidelines and Procedures (FOP- Treasury No. 101.2)
- Information Security Incident Response Plan (refer to OIIT policy and procedure manual)

OIIT policies and procedures, including PCI-DSS related matters, are maintained by OIIT and are available on the OIIT website.

Timeline

Effective Date:	Effective upon Approval
Review Date:	Within one year from the effective date.
Revised Date:	June 23, 2017

Approval

Approved by the President for adoption July 1, 2012