NC STATE UNIVERSITY

University Controller's Office
Internal Administrative Policy & Procedures

Section: General Accounting
Function: Cash Management
Person Responsible: Heidi Kozlowski

Procedure Number: *GA-CM-MS-02*
Procedure Title: Applying for a Merchant Account

History: Issued: April 2004; Revised March 2014

Purpose: Instructions for applying for and maintaining a merchant account

Procedures: The University Controller's Office is responsible for administering the process for accepting payments via credit card. This process is conducted in accordance with NCSU's participation in the State of North Carolina's Master Service Agreement (MSA) for payment card services and PCI-DSS requirements.

Merchant application process steps:

1. In order for a department to be able to accept credit card payments, they must obtain receipt center approval from the University Controller or designee. A form BA-114 Request/Authority to Establish Receipt Center needs to be completed and forwarded to the Controller or designee for review and approval. The forms can be downloaded from the Controller's Office home page: http://www.fis.ncsu.edu/controller/forms/default.asp.

2. Once approved as a receipt center, Contact Merchant Services Section at the Controller's Office to discuss the line of business, description of transactions, capture acceptance methods (Payment Applications, Payment Gateways, Point-of-Sale Terminal, etc), volume of business, go-live

3. Complete merchant application form, Request for Credit Card Outlet Authorization.

4. Upon acceptance as a merchant, the Merchant Service Section at the Controller's Office will provide installation/setup and training

5. PCI compliance evaluation and monitoring will be discussed with the merchant and will be

continual while the merchant account remains active.

Timeline for creating a Merchant Account

A merchant account can take a minimum of six weeks to complete from the initial meeting until the account is in production and the first transaction has been accepted.

Payment Processing Service

All University merchants are set up through the State of North Carolina's Master Service Agreement (MSA) with SunTrust Merchant Services (STMS), a partnership between SunTrust Bank and First Data Merchant Services (FDMS). STMS provides merchant card payment processing services. The North Carolina Office of the State Controller (OSC) has mandated that all agencies and universities of the State use the MSA unless an exemption has been approved. A University department may request an exemption from this requirement by providing a business case justifying an alternate vendor or process to Merchant Services in the Controller's Office. The business case will be reviewed by the University and the State Treasurer's Electronic Commerce Section. If approved, the Merchant Service Section will work with the department to implement, monitor, and maintain security and compliance in accordance with University policy over the alternate vendor.

University departments shall not enter into an outsourcing agreement with a third-party provider, including software applications for credit card processing, without prior approval.

Outsourcing Credit Card Payments

The University is required to participate in the Master Service Agreement (MSA) for merchant services provided by OSC due to Cash Management Law (General Statute 147-86.10 and 11). An exemption from participating may be obtained from OSC if a suitable business case is presented. (See Payment Processing Service).

This requirement applies to all contracts, including outsourced functions if they involve credit card processing. The requirement does apply even when the University is not the merchant for the credit card processing.

Any area of campus involved in or negotiating an outsourcing agreement that involves

processing credit cards through a processor not under the MSA should forward an exemption request to Merchant Services. (See Payment Processing Service).

Payment Gateway

NelNet is the University's preferred payment gateway and is required to be used for all internet credit card transactions. A University department may request an exemption from this requirement by providing a business case justifying an alternate vendor or process to Merchant Services. The business case will be reviewed and forwarded as appropriate to the PCI Team to request approval. A University department shall not enter into an outsourcing agreement with a third-party provider, including software applications for credit card processing, until the business case is approved. Upon approval, standard purchasing policies apply. Please see Merchant Procedure regarding The University's Payment Gateway, Nelnet for more information.

Complete Setup Forms

Once the department has completed the initial meeting with Merchant Services and decided on the capture method, the appropriate setup forms and documents must be completed. Merchant Services Section will identify the appropriate PCI Self Assessment (SAQ) questionnaire to be completed and the department will need to provide a workflow diagram and description. These forms are reviewed and approved by the Merchant Services Section and PCI Team. Once approved, the forms are submitted to the NC Office of the State Controller to be reviewed and sent to SunTrust Merchant Services for setup. The requesting department must complete PCI DSS training prior to 'go live' of the merchant account.

Credit Card Transaction Process

Method 1: Payment Gateway

The credit card transaction process begins when the customer purchases a product/event or makes a donation through a third party hosted payment application/website. This application website has a "Pay Now" button and passes the customer to the hosted payment gateway to make the payment. The payment gateway interfaces with the payment processor. The payment processor interfaces with the credit card companies to validate the credit card and verify the address if address verification is used. The payment processor returns an

authorization code to the payment gateway and settles the funds with the University's bank account.

Method 2: Point-of-Sale Terminal

The credit card transaction process begins when the customer purchases a product/event or makes a donation and their card is swiped or entered into a point-of-sale terminal. The terminal is connected through an analog or cellular telephone line to the payment processor for settlement. The payment processor interfaces with the credit card companies to validate the credit card and verify the address if address verification is used. The payment processor returns an authorization code to the point of sale terminal and settles the funds with the University's bank account.

Merchant Training

University departments approved as merchants shall ensure that all employees involved in the merchant service/credit card environment have completed the PCI trainings on an annual basis. These training sessions apply to any who participate in the merchant's payment process. These training sessions also apply to IT support/developers of applications and software that access or process credit card information or interface with credit card payment gateways. University departments shall also provide necessary training to employees to ensure staff members adhere to the policies and procedures for merchant services.

Currently, there are two online PCI training courses available that have developed by NCSU Security & Compliance. Merchants will be registered during the application process for these courses and are required to complete them prior to 'go live' of the merchant or if a new user to an existing merchant, the training must be completed before handling any credit card information.

The courses titled "Demystifying PCI" and "Completing SAQ questionnaire" should be completed by the following:

1. The individual who completes the annual Self-Assessment Questionnaire.

2. Individuals who are the IT support of servers, payment applications and software.

PCI Compliance Assessment

During the set up phase, the merchant needs to begin assessing their initial Payment Card Industry (PCI) Data Security Standard (DSS) Compliance. Assessment consists of the following steps:

1. Complete Initial SAQ – Before the merchant may begin accepting transactions, the merchant must complete their initial SAQ. The merchant should consult with Merchant Services, as required to verify which SAQ is applicable.

2. Review PCI DSS Requirements – After completing the initial PCI DSS SAQ, review PCI DSS to make sure that the merchant meets all applicable requirements. PCI Compliance is not a point-in-time, but a continuous day-to-day process.

3. Complete Compliance Documents - Merchants are required to have documented procedures for their business process related to credit card processing. A workflow diagram is a component of their documents.

Related Information:

Merchant Services Policy

Merchant Funding Policy

Contact Information:

University Controller's Office

Merchant Services

Campus Box 7205

Raleigh NC 27695-7205

merchantservices@ncsu.edu

Persons Involved in These Procedures:

Name of Person	Description of Duties
Merchants	Meet requirements and complete application.
Merchant Services	Review and approve merchant application. Complete OSC application and facilitate application process thru OSC.
Security & Compliance	Evaluates, monitors, and reports for PCI compliance.

Internal Administrative Procedures Approved By:

Name of Person	Date
Associate Controller: Heidi Kozlowski	November 26, 2007
University Controller:	