NC STATE UNIVERSITY

University Controller's Office
Internal Administrative Procedures

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

Procedure Number: GA-CM-MS-07
Procedure Title: Maintaining Payment Card Industry (PCI) Compliance

History: March, 2014

Procedures:

At all times, merchant accounts must be compliant with all applicable Data Security Standards (DSS) for their method of payment acceptance. Maintaining Payment Card Industry (PCI) compliance is not a point-in-time, but a continuous day-to-day process. The following policies and procedures will help ensure that cardholder data and the electronic commerce network are continuously protected and kept secure.

Daily

1. Never accept merchant's credit card information via email or email it to other departments.

2. Credit card merchants cannot store credit card information on a local computer or server.

3. Do not store the Card Identification Number (CID) electronically or on paper. The CID number is the three digit security code on the back of the credit card.

Quarterly

1. Perform internal and external vulnerability scans of all in-scope systems and remediate all high ranked vulnerabilities.

2. Change passwords for accounts that allow access to the cardholder data.

3. Verify that stored cardholder data is still needed and preferably not being stored beyond 60 days but not longer than 180 days.

Annually

Merchants must validate their PCI compliance annually by completing the following steps:

1. Review current PCI DSS regulations that are required for your merchant level. Contact

Merchant Services in the Controller's office for additional information.

2. If you are using a third party vendor, they must be a level one service provider and ensure their applications and systems are PCI compliant. Request their service provider certificate for PCI PA-DSS or the executive summary report of PCI DSS compliance.

3. All merchants must complete the annual PCI Compliance training through the Controller's Office.

4. Fill out the appropriate Self-Assessment Questionnaire (SAQ) and establish the policies and processes that are required by the SAQ. Send the completed SAQ and any process changes to Merchant Services in the Controller's office.

It is the responsibility of the Merchant to maintain PCI DSS compliance at all times. Failure to operate compliantly will result in the termination of the Merchant account and loss of accepting credit card payments.

Internal Administrative Procedures Approved By:

Name of Person	Date
Associate Controller: Heidi Kozlowski	April, 2014
University Controller:	