THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

VICE CHANCELLOR FOR FINANCE AND ADMINISTRATION

300 SOUTH BUILDING
CAMPUS BOX 1000
CHAPEL HILL, NC 27599-1000

TEL: 919-962-3795
FAX: 919-962-0647
www.unc.edu/financeadmin

MEMORANDUM

To: Deans, Directors, and Department Chairs
CC: Business Managers, ISL, CTC, ITD, & CC Adm Listservs

From: Karol Kain Gray, Vice Chancellor for Finance and Administration Karol Kain Gray
Chris Kielt, Interim Vice Chancellor for Information Technology and CIO

Subject: Compliance with Credit Card Processing Standards and Payment Gateway Update

DATE: February 11th, 2013

The University is committed to safeguarding personally-identifiable information including payment card data. To ensure the security of payment card data, all University departments must comply with the Payment Card Industry (PCI) Data Security Standard (DSS). PCI DSS is a mandatory security standard enforced by a contract with the University's payment card processor in addition to State and University policies. Failure to comply with PCI DSS may result in material fines and loss of the University's ability to process credit cards. Accordingly, any campus merchant accepting payment cards must conform to the regulations and take all necessary steps to be compliant if the unit wishes to continue to accept credit cards for payment.

For more information and tools pertaining to campus merchants and PCI DSS compliance, please visit:
http://finance.unc.edu/university-controller/merchant-card/resources.html

Acting on the requirements for PCI compliance, the following changes will take effect immediately.

1. The University is developing a centralized restricted cardholder data environment (CDE) in order to become PCI compliant with our external agreements. The CDE is an additional network that segregates cardholder data from the University's main network. Development of this CDE will require coordination between ITS and existing campus merchants.

2. Campus merchants will be required to use uPay and the TouchNet payment gateway. This will provide the University with a centralized and PCI compliant CDE for credit card transactions, and will also reduce overall compliance costs. All campus merchants currently utilizing a different payment gateway must migrate to TouchNet upon expiration of their current contract or prior to renewal. Requests for exemptions to this policy may be granted only with valid documented business reasons that are submitted to and approved by the CERTIFI committee.

3. To encourage the use of one payment gateway, campus merchants that use TouchNet will no longer pay the $0.55 per transaction fee. This cost will now be centralized and paid for by the University.

In addition to the above requirements, each campus merchant must address the following issues:

1. Complete annually the appropriate PCI Self-Assessment Questionnaire (SAQ) using the online compliance tool TrustKeeper. This has been made available at no cost to the campus merchant.

2. Workstations used to process credit card transactions cannot be used for any other purpose (internet use, email, etc.)

3. Discontinue email use for any communication and processing of cardholder data.

4. Maintain an inventory of all devices in the cardholder data environment (CDE).

5. Physically secure computers and Point of Sale (POS) terminals used for credit card processing to avoid compromise.

6. Review credit card document management and the secure storage procedures along with retention policies. These documents are currently being updated and will be made available within the next thirty days.

7. Each campus merchant is required to document departmental procedures and workflow of the card holder environment (CDE) including all possible transaction scenarios, from start to finish. These documents should be reviewed annually with departmental personnel and updates provided as needed.

8. Require all staff involved with credit card processing to complete PCI training on an annual basis. Online training via Vigitrust has been made available at no cost to the campus merchant.

As a reminder to all business units, any contracts related to credit card acceptance need to be reviewed by the CERTIFI committee **before** signing to ensure University policies (including PCI Compliance) are being met. This includes but is not limited to software or hardware purchases, upgrades, renewals, and outsourcing credit card payments to a vendor. The CERTIFI committee review will cover areas such as the PCI compliance status of the vendor and workflow consistent with the University's role in supporting credit card merchants.

Given the compliance, security, and complexity issues of credit card merchant processes, the CERTIFI committee is charged with the overall responsibility of electronic receipts on campus. If your campus unit is planning to establish and/or modify a credit card merchant process, including any form of outsourcing, the University's Merchant Card Accountant must be contacted at 962-7792 or certifi@unc.edu and approval must be obtained by the CERTIFI committee before a system is purchased or developed. The above would also apply to contracts or software that contain electronic payment capabilities.

The CERTIFI committee is co-sponsored by the Finance Division and Information Technology Services with members being selected to represent a knowledge base versed in credit card merchant compliance, systems technical skills, information security, University and Office of the State Controller policies, and electronic commerce. A list of the current members of the CERTIFI committee may be found at: http://finance.unc.edu/images/stories/committee/certifi_members_2012.pdf

We greatly appreciate your efforts in meeting the PCI compliance standards.