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

From: Richard L. Mann, Vice Chancellor for Finance and Administration
Larry Conrad, Vice Chancellor for Information Technology and CIO

Re: Policy and Information Security for Credit Card Merchant Services

Date: September 16, 2011

University Policy 308, *Credit Card Merchant Services*, has been updated to provide additional guidance on the acceptance of credit cards to receive payment. University departments provide goods and services to its customers and may accept credit cards as an appropriate form of payment. Many University departments have been set up with credit card merchant accounts consisting of point of sale (POS) terminals and customized internet applications. The purposes of the updated credit card merchant policies and procedures are:

- to provide essential information in obtaining and managing merchant accounts for credit card receipts,
- to provide requirements to ensure proper control and integrity of credit card data as well as security in the collection, maintenance, and transfer of credit card data, and
- to ensure compliance with the standards of the leading card associations referred to as the Payment Card Industry (PCI) Data Security Standard.

Several factors led to the update of University Policy 308. There has been a significant increase in the use of credit cards to receive payments, especially for processes using internet applications. The NC Office of the State Controller (OSC) is statutorily charged with administering the State's electronic commerce program, which includes credit card merchant services, and has issued new policies and entered into contractual agreements which impact our campus processes. Also, the PCI Data Security Standard applies to our campus departments that accept payments by credit cards. **The University must be compliant with the new PCI Data Security Standard 2.0 effective January 1, 2012.**

The primary focus of the PCI Data Security Standard is to help merchants (such as University departments) improve the security of cardholder information by improving overall security standards which reduces the chances of security breaches. The growth of electronic commerce has resulted in increased occurrences of stolen cardholder information throughout the industry, which is an important

concern to merchants and others that rely on electronic commerce as an efficient payment method.

The rise in cardholder information compromises has resulted in an increased focus and regulatory actions by the major card associations. To improve the integrity and security of the payment processes used for receipt of payments by credit cards, compliance with the PCI Data Security Standard is necessary. The standard helps merchants improve the safekeeping of cardholder information, which in turn reduces the chances of security breaches, fraud, and potential financial losses. These policies and procedures will help ensure that cardholder data and the electronic commerce network are protected and kept secure.

ITS and the Finance Division have worked collaboratively to attain compliance with industry standards, OSC policies, and sound business principles. The updated policy for credit card merchant services will help our campus maintain this compliance. The policy and related procedure are available in the Finance Policy and Procedure Manual.

Given the compliance, security, and complexity issues of credit card merchant processes, the CERTIFI (Compliant Electronic Receipts Through Innovation and Financial Integrity) Committee was 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[1], the University's Cash Manager must be contacted at 962-1601 or ccadmin@unc.edu and approval must be obtained by the CERTIFI committee before purchase or development. The above would also apply to contracts or software that contains electronic payment capabilities.** In order to receive communications regarding PCI Data Security Standard 2.0 compliance and other credit card merchant issues, it is important to verify with the University's Cash Manger that identified personnel are subscribed to the credit card administrator listserv.

Mandatory, online annual credit card merchant security awareness training through Vigitrust has been made available to address the security awareness obligation of the PCI Data Security Standard. **In addition, mandatory classes will be held this fall for campus credit card merchants. These classes will provide detailed instructions on maintaining PCI compliance under the new PCI Data Security Standard 2.0.** Registration information regarding the training class is available on the Finance Division website under training. Individual meetings with credit card merchants required to answer SAQ-D questionnaires will be held since they have likely the most significant work ahead of them for PCI Data Security Standard 2.0 compliance. These meetings will also be mandatory.

Thank you for your continued support toward overall compliance and credit card data security.

cc: Business Managers Listserv

[1] Includes outsourcing or any modification that may impact information security of the merchant's credit card process.