DoIT 01 08 - University Acceptance of Credit or Debit Cards

*October 9, 2009 Archived version (Effective October 9, 2009 through June 22, 2014)*

Authority: Statewide Information Security Manual, ISO 27002 15.1.4,

History: First issued April 24, 2008. Last revised October 9, 2009.

Related Policies:

Additional References: PCI Security Standards Council document library. https://www.pcisecuritystandards.org/security\_standards/documents.php

http://www.uncp.edu/doit/policies/UNCP\_PCI\_Data\_Security\_Standard\_Procedure.html

Contact Information: Vice Chancellor for Information Technology and CIO, (910.521.6883)

1. Purpose

1.1 The University of North Carolina at Pembroke accepts credit or debit cards for payment of goods and services under controlled conditions to protect against the exposure and possible theft of account and personal cardholder information that has been provided to the university; and to comply with Payment Card Industry Security Standards Council (hereinafter “PCI”) requirements which became effective June 30, 2005. The university must adhere to these standards to continue to process payments using payment cards.

2. Scope

2.1 This policy applies to all UNC Pembroke departments and affiliated units, employees, contractors, consultants, temporaries and other workers. This policy is applicable to any unit that processes, transmits or handles cardholder information in a physical or electronic format. The PCI Data Security Standard governs all computers and electronic devices at UNCP involved in processing payment card data. This includes servers that store payment card numbers, workstations that are used to enter payment card information into a central system (for example, ordering tickets over the phone), and any computers, network devices or credit/debit card swipe devices through which the payment card information is transmitted.

3. Definitions

3.1 PCI Data Security Standard (PCI DSS**)** – a document that defines the standards for secure processing, storage and transmission of payment card data. The standard is a result of collaboration among several large credit card brands. Each brand has its own standard similar to the PCID SS.

3.2 PCI Security Standards Council – an industry association whose purpose is to improve security of payment card data and foster support and adoption of the PCI Data Security Standard and related standards.

3.3Payment Card – a credit or debit card.

3.4 Cardholder data – any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, and address, social security number or Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data).

3.5Merchant– any person or department accepting money for goods or services, including conference registrations, memberships, fees, etc.

3.6Merchant Outlet ID – a unique id assigned to identify transactions specific to a merchant.

4. Policy

4.1 All transactions that involve the transfer of payment card information must be performed on systems jointly approved by the Offices of the Controller and the Division of Information Technology (DoIT). Said systems must pass an internal compliance and security review before payment processing begins. Any specialized servers or related equipment that have been approved for this activity must be housed in a protected, managed network that meets the full requirements of the PCI DSS. The Division of Information Technology must approve this network before operations begin and review yearly as long as the network is in use. The network must be administered in accordance with the requirements of all UNCP policies and the PCI DSS.

4.2 Departments involved with the acceptance and processing of cards for payment of goods and services must design adequate processes to ensure the following requirements are met continuously:

4.2.1 Approval of the Offices of the Controller and the Division of Information Technology must be obtained before entering into any contracts, purchases of software and/or equipment or purchases of any processing services related to payment card processing. This requirement applies regardless of the transaction method or technology used (e.g., e-commerce, point-of-sale (POS) device, etc.).

4.2.2 Departments must comply with the [Payment Card Industry Data Security Standard](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf) as it may be amended from time to time.

4.2.3 Departments must establish procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions regardless of whether initiated via the telephone, over the counter, mail order, Internet, etc. Departments must ensure compliance with UNCP’s Personal Information Security Breach Notification Protocol (DoIT 07 07) for notifying cardholders in the event of improper disclosure of personal identifying information.

4.2.4 Credit or debit card numbers must not be transmitted in an insecure manner, such as by email, unsecured or stored fax or through unsecure campus mail (sealed envelopes must be used). Under no circumstances will it be permissible to obtain payment card information or transmit payment card information by email.

4.2.5 Sensitive cardholder data [i.e., full account number, card type, expiration, PIN and card-validation code (three-digit or four-digit value printed on the front or back of the card)] should not be stored in any university system, personal computer or email account, nor should this data traverse UNCP’s network.

4.2.6 Departments should not print the entire credit or debit card number on the customer copy of any receipts. Whenever possible, departments should not print the entire credit or debit card number on the department’s copy of the receipt.

4.2.7 All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers and safes, with limited access to only individuals who are processing the payment card transaction. Processing should be done as soon as possible and the payment card number should immediately be blacked out to the last four digits and the card expiration date must be masked.

4.2.8 Access to payment card data should be limited to those individuals who need access in order to perform their job duties. Access should be removed promptly when no longer required to perform current job duties.

4.2.9 Stored payment card information will be retained according to the University General Records Retention and Disposition Schedule and any requirements as set forth by the Office of the State Controller or the Office of the State Auditor. All media used for payment cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.

4.2.10 Criminal background checks must be performed prior to hiring of any new employee with access to stored cardholder information for multiple cards. This is not required for positions that only handle one card at a time, and do not have access to stored card data. Background checks must be carried out as established in Human Resources policy.

4.2.11 Payment card handlers and processors must sign a written acknowledgement stating their understanding of their obligation not to disclose or acquire any information concerning a cardholder’s account without the cardholder’s consent, and to follow all PCI DSS requirements.

4.2.12 All personnel involved in payment card handling must attend card security training provided by the Offices of the Controller and the Division of Information Technology every year in conjunction with required PCI DSS reviews. New employees must attend this training prior to accessing payment card data.

4.2.13 Each department using servers or similar equipment must develop procedures to ensure that access privileges are controlled, software can only be accessed and used in secure locations, and access for former employees is promptly removed.

4.2.14 Units using third-party software, including cash register systems, are prohibited from storing complete payment card numbers on university computers at any time.

4.2.15 Departments must contractually require all third parties with access to cardholder data to adhere to all PCI security requirements and provide proof of PCI certification to the Offices of the Controller and the Division of Information Technology. This certification may be required periodically in order to meet review and reporting needs.

4.2.16 Any member of the campus community, including faculty, staff, students, temporary workers, contractors, etc., must report any violation of this policy to the Offices of the Controller and the Division of Information Technology as soon as possible.

4.2.17 The Offices of the Controller, Internal Audit and the Division of Information Technology may periodically review and assess the business processes and technology used to process payment card data in order to comply with PCI DSS requirements and those of the Offices of the State Controller or State Auditor.

5. Procedures

5.1 Any department wishing to enter or renew a credit card and/or debit card processing contract must provide the Offices of the Controller and the Division of Information Technology all relevant information related to the intended use of card processing and the technical specifications for said processing. Because the sale of goods and services to entities outside the university community may raise special considerations (e.g., unrelated business tax, accounting, legal, etc.) business plans concerning card sales should also be reviewed by the Controller’s Office.

5.2 Upon approval by both offices, and at the discretion of the Office of the Controller, a specialized Merchant Outlet ID will be established for use by the department. The department will work with the Controller’s Office and the Division of Information Technology to review their application and Web site, and to integrate the payment mechanism into campus systems. The Office of the Controller will establish the accounting practices that must be followed during payment processing and reconciliation.

5.3 Departments that need to accept credit/debit cards through a physical terminal or a swipe device must contact the Offices of the Controller and DoIT to execute the required paper work, obtain a Merchant Outlet ID, receive training, and be given direction as to the accounting of those transactions. All equipment must meet PCI DSS requirements.

5.4 Following review and approval, the department will be notified of the status and additional relevant information. The Office of the Controller must approve any subsequent changes in processes for handling payment card data before such processes are put into effect. The Division of Information Technology must approve any subsequent changes in the technology before such changes are put into effect. The changes that must be approved by the Controller’s Office or DoIT include, but are not limited to, changes to the department Web site, products or services to be sold, intended customer base, anticipated transaction volume, outside advertising, application software, or changes in the departmental contacts responsible for the e-commerce business plan.

6. Sanctions

6.1 Departments not complying with this policy may lose the privilege to serve as a payment card merchant. Additionally, the affected card company may assert authority to impose fines, beginning at $100,000 for the first violation. Other civil liabilities may exist as well.

6.2 Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The university will carry out its responsibility to report such violations to the appropriate authorities and may prosecute any such violations to the full extent of the law.

7. Resources

[PCI Data Security Standard and related documents](https://www.pcisecuritystandards.org/tech/supporting_documents.htm)