05.118 Credit Card Acceptance Policy

Authority: Vice Chancellor of Business Affairs

History: Effective July 1, 2011
Updated February 2013

Source of Authority: Office of State Controller (OSC); Office of State Budget and Management (OSBM); Payment Card Industry (PCI) Data Security Standards; NCGS §66-58.12

Related Links: Credit Card Acceptance Procedures; Departmental Funds Receipting Policy and Procedures; PCI Council's website; additional resources and policies are located at the Office of State Controller's web site

Responsible Office: Controller

I. Purpose

University of North Carolina Wilmington accepts merchant cards as an acceptable form of payment. This policy is to provide the administrative, technical and security standards that must be adhered to in order to ensure compliance with applicable rules, regulations and policies associated with merchant cards.

II. Scope

Applies to all university departments or activities.

III. Policy

A. Receipts and Cards Accepted

1. Receipts Accepted: University departments that have received approval under the UNCW Departmental Funds Receipting Policy (see related links) may accept merchant cards for allowable goods or services. Approval for the acceptance of merchant cards must be obtained from the Vice Chancellor for Business Affairs or assigned delegate.

2. Cards Accepted: University departments may accept MasterCard, VISA and American Express. Only VISA and MasterCard are accepted for student account transactions.

B. Transaction Fees

Transaction fees (convenience fees) are levied and retained by a third-party vendor for credit card transactions made online to the student account.

C. Funding to Pay Costs

University departments shall adhere to all requirements pertaining to the securing of funding to pay for costs associated with processing merchant cards, including internal costs and costs paid to third-party processors.

D. Methods of Capture

The following methods of capture are allowable:

1. Internet application – hosted by university Internet application – hosted by third-party

2. Third-party gateway for processing transactions

3. POS terminals – Stand-alone (Analog telephone lines)

4. Telephone orders

5. Mail orders

E. Third-Party Service Providers

1. Merchant Card Processing Services

   Merchant card payment processing services to state and local government entities (including UNCW) is on a statewide enterprise basis via an outside vendor.

2. Payment Applications

   Capture solutions utilizing POS Software applications are obtained from vendors that have had the application (version utilized) validated as being compliant with the PCI Payment Application Data Security Standard (PCI PA-DSS), formerly known as Visa's "Payment Application Best Practice" (PABP). The payment application must be listed either on Visa's "List of Validated Payment Applications or on the PCI Council's website (see Related Links above).

F. Data and System Security

1. PCI DSS Compliance

   a. Payment Card Industry Data Security Standard (PCI DSS)

The university will take all necessary steps to ensure that all merchant card applications (merchant numbers) used by the university are kept compliant with the "Payment Card Industry Data Security Standard (PCI DSS)," which has been issued by the PCI Security Council to help ensure that cardholder data and the electronic commerce network are protected and kept secure, thereby avoiding potential fines. The university will advise the OSC and keep it updated with, the name of the university's PCI contact.

b. Self-Assessment Questionnaire

An annual Self-Assessment Questionnaire (SAQ) provided by UNCW's vendor will be conducted annually by the UNCW IT Security Officer in collaboration with the university's PCI coordinator in the Controller's Office.

c. Third-party Capture Application

The third-party capture application must be and remain compliant with the PCI PA-DSS. It must be listed on Visa's CISP website or on the PCI Security Council's website as a "Validated Payment Application." Default passwords are not used. The software is updated within 30 days of the release of any security patches.

d. Third-party Gateway Vendor

The third-party gateway vendor, functioning as a "service provider", must be and remain PCI DSS compliant. A "written agreement" must be in place with the vendor that specifies the vendor's PCI data security responsibilities. The written agreement language is contained in the original contract. The university must monitor the vendor's compliance on an ongoing basis. Evidence of compliance will be obtained from the gateway service provider annually and maintained by the Controller's Office.

e. Response to Issues

Issues detected by either the Self-Assessment Questionnaires (SAQ), or by vendor's vulnerability scans, or by failure of the service provider to demonstrate compliance, will be brought to the attention of the Vice Chancellor of Business Affairs and Vice Chancellors of Information Technology Systems Division. A plan for remediation will immediately be developed for each incident of non-compliance detected, and the Office of the State Controller will be advised.

f. UNCW shall adhere to the following PCI DSS requirements:

1) Build and maintain a secure network
   a) Install and maintain a firewall configuration to protect cardholder data

b) Do not use vendor-supplied defaults for system passwords and other security parameters

2) Protect Cardholder Data
   a) Protect stored cardholder data
   b) Encrypt transmission of cardholder data and sensitive information across public networks
3) Maintain a vulnerability management program
   a) Use and regularly update anti-virus software
   b) Develop and maintain secure systems and applications
4) Implement strong access control measures
   a) Restrict access to cardholder data by business need-to-know
   b) Assign a unique ID to each person with computer access
   c) Restrict physical access to cardholder data
5) Regularly monitor and test networks
   a) Track and monitor all access to network resources and cardholder data
   b) Regularly test security systems and processes (i.e. annual penetration tests, which are different than the vulnerability scanning requirement)
6) Maintain an information security policy
7) Compensating controls may be a consideration if a requirement cannot be met due to legitimate technical or documented business constraints.

2. System Security Requirements for Merchant Card Services

The university will incorporate the following requirements into its processing of merchant cards.

a. System Settings

1) Change vendor default security settings prior to installing the system on the network

2) Disable or change default accounts and passwords prior to installing the system on the network

3) Harden production systems by removing all unnecessary services and protocols

4) Use secure, encrypted communications for remote administrative access

b. Stored Data Protection

1) Dispose of sensitive cardholder data when it is no longer needed

2) Do not store the full contents of any track from the magnetic stripe in any manner

3) Do not store the card-validation code (the three digit value printed on the signature panel of a card) in any manner

4) Mask all but the last four digits of the account number when displaying cardholder data

5) Accounts numbers must be securely stored by means of encryption or truncation

6) Account numbers must be sanitized before being logged in the audit trail

7) Access to card account numbers must be restricted for users on a need-to-know basis.

c. Transmitted Data Protection

1) Transmissions of sensitive cardholder data must be encrypted through the use of SSL

2) Credit card numbers must not be transmitted via email

d. Anti-Virus Protection

All Microsoft Windows Servers and workstations must have antivirus software installed and the virus definitions must be updated regularly.

e. Applications and Systems Security

1) All networks will be established in accordance with the firewall configurations as specified by the PCI DSS

2) All systems must be updated with the latest security patches within 30 days of their release

3) The software and development process must be based on industry best practice and information security must be included throughout the process

4) Sensitive cardholder data must be sanitized before it is used for testing and development

5) All changes must be formally authorized, planned and logged

6) Sensitive cardholder data stored in cookies must be secured or encrypted

f. Account Security

1) All users must authenticate using a unique user ID and password

2) Remote access must be via a secure connection

3) All passwords must be encrypted

4) All user accounts must be revoked immediately upon termination

5) All user accounts must be regularly reviewed to ensure that malicious, out-of-date and unknown accounts do not exist

6) All inactive accounts must be automatically disabled after a pre-defined period

7) Vendor accounts used for remote maintenance must be disabled when not needed

8) Group, shared or generic accounts are prohibited

9) Passwords must be changed at least every 90 days

10) Passwords must follow strong password conventions

11) Multiple password attempts or brute force attacks must result in an account lockout

g. Physical Access

1) Multiple physical security controls must prevent unauthorized access to the facility

2) Equipment and media containing cardholder data must be physically protected against unauthorized access

3) Cardholder data printed on paper or received by fax must be protected against unauthorized access

4) Proper procedures for the distribution and disposal of any media containing cardholder data must be followed

5) All media devices that store cardholder data must be inventoried and properly secured. The merchant copy of receipts shall be kept for a minimum of 18 months. (Retention should be included in agency's official records retention schedule.)

6) Cardholder data must be deleted or destroyed before it is physically disposed (e.g. by shredding paper and degaussing media)

7) All cache containing merchant card data must be cleared daily.

h. Access tracking

1) All access to cardholder data must be logged

2) Logs must contain successful and unsuccessful login attempts and all access to the audit logs

3) Critical system clocks must be synchronized with the agency's time server, and logs must include date and time stamps

4) Secure logs are maintained by vendor.

i. Security breaches – Incident Plan

The university shall adhere to all requirements pertaining to the establishment of a security incident plan as required by the PCI Data Security Standard and other applicable policies. This includes any actions necessary to secure any exposed data, to report the incident to appropriate management, to report the incident to the Office of the State Controller, and adhering to applicable statues, including the NC Identity Theft Protection Act.

G. Training

As specified by the PCI DSS, all employees having access to merchant card data must be advised of the expectation of being aware of the sensitivity of data and their responsibilities for protecting it. Each department within UNCW acting as a merchant shall ensure that all employees responsible for systems or procedures related to merchant card transactions or data will be provided proper training relating to the policies and procedures for merchant card processing, including being provided a copy of this policy document. Each employee will be required to acknowledge in writing that they have read and understood the applicable security policies and procedures. Additionally, all employees will be advised to refer to the State Controller's SECP Website on a frequent basis to ascertain any changes or advisements. Most resources can be found on the State Controller's SECP Website.