Payment Card Processing Compliance

REG07.60.01 Current Version

Authority: Chancellor

History: Placed in University Policy Manual after EXPEDITED REVIEW, transitioned without substantive change from prior version, March 25, 2013; updated July 16, 2013.

Related Policies:

Additional Resources: East Carolina University Payment Card Industry (PCI) Standard Statement

East Carolina University PCI Security Awareness for Campus Credit Card Merchants

PCI Security Standards Council PCI Security Standards

North Carolina Office of the State Controller PCI Security Compliance Program PCI Security Compliance Program

Contact Information: eCommerce Manager, 737-4729, ecommerce@ecu.edu

1. Purpose

The purpose of this regulation is to ensure the security of all payment card holder data as it relates to all practices at East Carolina University.

2. Introduction and Background

The Payment Card Industry Security Standards Council, founded by all of the major credit card companies, has created a set of standards

formally know as the Payment Card Industry Data Security Standard (PCI DSS). The intention of the PCI DSS is to help merchants ensure the security of payment card data by improving overall business practices thus reducing the likelihood of a security breach. The PCI DSS contains requirements necessary for the secure collection, transmission, processing and storage of payment card data. All credit card merchants must incorporate the PCI DSS into their business practices in order to retain credit card processing privileges with their respective credit card companies.

The North Carolina Office of the State Controller (OSC) is charged with ensuring that all state agencies adopt and comply with the PCI DSS. East Carolina University, its campus payment card merchants and their agents must adopt and comply with the PCI DSS in order to retain credit card processing privileges as members of the Master Services Agreement that is provided by the OSC.

3. Definitions

3.1 Payment Card , Includes credit cards, debit cards, ATM cards, and any other card or device other than cash or checks, issued by a bank or credit union, which is normally presented by a person seeking to make payment, for the purpose of making a payment.

3.2 Payment Card (Cardholder) Data - A Payment Card holder,s name and contact information, Payment Card number, account number, card expiration date, CVV2, CVC2, Payment Card transaction information and/or any other information that may be used to personally identify a Payment Card account or holder.

3.3 CVV , Card Verification Value or Code. Three or four digit number on the front or back of a payment card used to verify card-not-present transactions.

3.4 Payment Card System - Any computing or information technology device, server, desktop computer, or other system used to access, store, process, or transmit Cardholder Data.

3.5 OSC - The North Carolina Office of the State Controller.

3.6 PCI DSS - Payment Card Industry Data Security Standard.

3.7 Locally hosted - Any Payment Card System using computing devices connected to the ECU network to store, process, access, transmit, or receive Cardholder Data.

3.8 Outsourced - Any Payment Card System using computing devices

located off the ECU campus to store, process, access, transmit, or receive Cardholder Data.

3.8.1 All vendors, networks, and software used in these systems must be certified PCI compliant.

3.8.2 Departmental workstations on the ECU network that connect to outsourced systems for the purpose of conducting Payment Card transactions must be located on a special area of the ECU data network called the ‚PCI VLAN, before connecting to the outsourced Payment Card system.

3.9 MDRP - Merchant Department Responsible Person designated as the individual within a department who will have primary authority and responsibility for Payment Card transaction processing within that department.

3.10 PCI VLAN - Virtual Local Area Network created to help reduce the risk of unauthorized access to sensitive Cardholder Data.

3.11 Visa Cardholder Information Security Program (CISP) , Information security program drafted by Visa and adopted by most major credit card companies.

4. Violation Consequences

4.1 East Carolina University is responsible for the loss or theft of payment card account information and non-compliance issues because all campus payment card merchants are operating under a chain merchant identification number belonging to the University. However, ultimate responsibility for losses, thefts or non-compliance and related fines and/or consequences lies with the merchant department in which a compromise or non-compliant incident occurs. Examples of fines and consequences are outlined below:

4.1.1 A confirmed or suspected compromise of payment card data must be reported immediately to the PCI Compliance Committee for submission to the proper payment card companies. A merchant failing to immediately report such a compromise risks a penalty of $100,000.00 per incident per CISP.

4.1.2 A merchant is subject to fines of up to $500,000.00 per incident per CISP if it is non-compliant at the time of a data compromise.

4.1.3 Merchant department payment card processing privileges may be suspended or revoked as a result of the loss or theft of payment card data or for non-compliance with the PCI DSS.

4.1.4 Merchant department employees may be subject to disciplinary action as a result of a deliberate violation or negligence of the PCI DSS.

5. Responsible Officers and Parties

5.1 The Vice Chancellor of Administration and Finance is responsible for ensuring that all ECU payment card activity is PCI DSS compliant. The PCI Compliance Committee, as a delegate for the Vice Chancellor of Administration and Finance, is responsible for creating policies and procedures, administering and monitoring payment card activity to ensure compliance with the PCI DSS.

5.2 The PCI Compliance Committee,s duties include, but are not limited to, the following:

5.2.1 Review New Payment Card Merchant Requests
5.2.2 Review Pending/Requested Changes to Existing Payment Card Systems
5.2.3 Approval/Denial Recommendations to ECU Financial Services
5.2.4 Administer and review Self Assessment Questionnaires Annually
5.2.4 University Education and Training on PCI DSS

6. Prohibited Activities

6.1 The storage of full payment card numbers on any device connected to the campus data network is prohibited.

6.2 Employees and existing merchants are prohibited from contacting the Office of the State Controller and SunTrust/First Data directly. All questions and inquiries must be directed to Robin Owens, eCommerce Manager.

6.3 Changes to an existing payment card system are prohibited without the prior approval of the PCI Compliance Committee.

6.4 ECU merchants are prohibited from using wireless data networks (like the ECU wireless data network) to send or receive payment card data.

7. Requirements

7.1 All payment card systems (including but not limited to software packages, hardware, services, etc.) must be reviewed by the PCI Compliance Committee and approved in writing by ECU Financial Services prior to purchase and/or implementation.

7.2 All ECU departments, employees and agents must adhere to all rules,

regulations and contractual provisions, including the PCI DSS and ECU policies and procedures regarding the secure handling of payment cards and payment card holder data.

7.3 Any ECU merchant department that wants to accept payments by payment card must submit a written request from its director, dean or department chair to the Director of Student Financial Services prior to accepting any credit card payments.

7.4 All merchant requests to accept payments by terminals or payment card systems must be reviewed by the PCI Compliance Committee and certified PCI Compliant by ECU Financial Services prior to accepting any card payments.

7.5 Online/Network Payment Card Systems that move or access Cardholder Data via the campus network must use the services of a University Authorized Vendor to process all Payment Card transactions.

7.6 All software, hardware, and vendors used in a PCI DSS compliant environment must be approved in writing by ECU Financial Services within 90 days prior to purchase of equipment/software/services or execution of contracts. All purchases must be executed in accordance with the ECU Basic Purchasing Procedures.

7.7 A merchant ID must be issued by the Office of State Controller before payment card payments can be accepted.

7.8 Changes to an existing payment card system must be presented to, and reviewed by, the PCI Compliance Committee and certified PCI compliant by ECU Financial Services prior to implementing the change. Change presentations must include signatures of the requestor and the department head of the requesting merchant department.

Changes to a payment card system include, but are not limited to, the following:

7.8.1 Payment gateway
7.8.2 Third-party vendor for hardware, software, or hosting services
7.8.3 Payment Card processing software versions (on server or workstation)
7.8.4 Location and physical access to servers or workstations
7.8.5 Network jack used to connect server or workstation to PCI-compliant section of ECU network.
7.8.6 Equipment upgrades, purchases, replacements, or modifications such as workstations or laptop computers

7.8.7 Software upgrades, purchases, replacements, or modifications
7.8.8 Payment card processing procedures

7.9 ECU Payment Card Data Security Program

7.9.1 All ECU payment card merchants must maintain continuous PCI DSS compliance.

7.9.2 Payment card policies and procedures drafted within ECU merchant departments must comply with PCI DSS and be formally documented in each department,s business manual.

7.9.3 Each ECU payment card merchant department must designate a contact person and a backup know as the Merchant Department Responsible Person (MDRP). The MDRP will serve as the liaison for the merchant department regarding payment card processing and PCI DSS issues.

7.9.4 The MDRP must facilitate the validation process by timely providing accurate information requested by the PCI Compliance Committee. This includes, but is not limited to, the completion of Self Assessment Questionnaires and Security Awareness documentation annually.

7.9.5 The MDRP will be responsible for educating the merchant department staff on PCI DSS compliance and related ECU policies and procedures.

7.9.6 Merchants are responsible for securing and retaining their vendor certificates of PCI DSS compliance and for requesting annual updates to such certificates.

7.10 ECU departments shall adhere to all applicable standards and procedures as specified in the ECU PCI Standard Statement and the ECU PCI Security Awareness for Campus Credit Card Merchants documents.