UNIVERSITY OF RICHMOND

Department: Treasury Services	**Effective Date:** July 24, 2013
Policy Number:	**Date Approved**: July 24, 2013
Policy Description: Policy for Payment Card Acceptance and Security	**Approved By:** Ecommerce Committee
Created: March 22, 2013	**Reviewed:** N/A
Cognizant University Official: David Hale, Vice President for Business and Finance	**Replaces Policy Dated:** October 12, 2007

PURPOSE:

This policy addresses Payment Card Industry (PCI) Data Security Standards (DSS) that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment. The policy covers the following specific areas contained in the PCI standards related to cardholder data: processing, transmitting, storing and disposing of cardholder data.

SCOPE:

This policy applies to the University of Richmond and all of its Affiliates. As used in this policy, the term "Affiliates" means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board.

POLICY:

Definitions

1) PCI-DSS - Payment Card Industry Data Security Standards – the security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands:
   - Visa
   - MasterCard
   - American Express
   - Discover
   - JCB (Japan Credit Bureau)

2) Card Holder Data (CHD) – Those elements of credit card information that are required to be protected. These elements include the Primary Account Number (PAN) in conjunction with:
   - Cardholder name

- Expiration Date
- Service code
- CVV/CVV2/CSC2

3) Disposal – CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices.

   The approved disposal methods for hard copy and paper documents are:
   - Cross-cut shredding
   - Incineration
   - Approved shredding or disposal service

   Before disposal or repurposing of electronic equipment, electronic equipment should be sanitized in accordance with the University of Richmond's Electronic Equipment Disposal Policy - http://is.richmond.edu/policies/technology/electronic-equipment-disposal.html.

4) Merchant Department – any department or unit (can be a group of departments or a subset of a department) which has been approved by the University of Richmond's Ecommerce Committee to accept credit cards and has been assigned a Merchant identification number.

5) Merchant Department Responsible Person (MDRP) – an individual (typically the manager) within the department who has primary authority and responsibility within that department for credit card transactions. The MDRP will complete the annual Self-Assessment Questionnaire for their merchant location.

6) Ecommerce Committee – A cross-functional team that evaluates and recommends compliant and cost-effective use of payment processes and systems at the University of Richmond. Members of the Ecommerce Committee consist of the following positions:
   - Assistant Vice President for Systems & Networks
   - Credit Card Manager
   - Information Services Security Administrator
   - System Administrator
   - Associate Bursar
   - Director of Treasury Services
   - Manager, Internal Audit
   - Application Administrator
   - User Services Manager
   - Assistant Vice President Telecommunications Multimedia Service
   - Three managers from merchant locations currently from Athletic Ticketing, Athletic Marketing and Retail Operations. Periodically, these positions will rotate off the committee and will be replaced by other merchant managers.

1.0 Statement of Policy

The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. The University of Richmond is committed to being in compliance with the PCI Data Security Standard as promulgated by the PCI Security Standards Council. Additionally, University of Richmond is committed to being in compliance with its Data Exposure Policy at http://is.richmond.edu/policies/general/data-exposure-policy.html.

2.0 Credit Card Acceptance and Handling

In the course of doing business at the University of Richmond, including affiliated organizations, it may be necessary for a department or other unit to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards is done on a case by case basis. Any fees associated with the acceptance of the credit card in that unit, will be charged to the unit. Fees for existing merchant accounts will continue to be charged according to current budget practices.

Departments or units that wish to establish a new cardholder payment process, system, or device must contact the Ecommerce Committee for evaluation and approval prior to signing of any agreement, issuance of purchase order or use. Departments that already accept credit and debit cards must contact the Ecommerce Committee for evaluation and approval prior to implementing an upgrade to the existing system, to changing the hardware or software or expanding an existing system. The Ecommerce Committee email address is: ecommerce@richmond.edu.

2.1 Steps for opening a new merchant account include:

a. Completion of an "Application for Payment Card Merchants"
b. Application approval
c. Read and accept this document, "Policy for Payment Card Acceptance and Security", in its entirety and ensure ongoing compliance with all requirements.
d. Training

2.2 Any department accepting credit cards on behalf of the University of Richmond must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions. This individual is referred to as the **Merchant Department Responsible Person** or MDRP. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the MDRP is unavailable.

2.3 Specific details regarding processing and recording credit card transactions to Banner will depend upon the method of credit card acceptance and type of merchant account. When the

merchant account is established, contact the Associate Bursar for cashier training.

2.4 Only PCI-DSS approved software and hardware may be used for processing credit cards. The Ecommerce Committee examines new credit card technology, on a regular basis, to determine if the technology (software and hardware) meets PCI data security standards.

3.0 Credit Card Data Security Policy

Procedures must be documented by authorized departments and be available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

3.1 Cardholder data collected is restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access and review the list monthly to ensure that the list reflects the most current access needed and granted. The MDRP is responsible for ensuring this is done and that it is tracked and documented on a monthly basis.

3.2 Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

3.3 All equipment used to collect data is secured against unauthorized use or tampering in accordance with the PCI Data Security Standard.
https://www.pcisecuritystandards.org/security_standards/index.php

3.4 All equipment and documents containing cardholder data must be kept in a secure, locked location.

3.5 Email should not be used to transmit credit card or personal payment information, nor should it be accepted as a method to supply such information.

3.6 Fax machines used to transmit credit card information to a merchant department, shall be a stand-alone machine with appropriate physical security.

3.7 No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card-validation code.

3.8 Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

3.9 Cardholder data (primary account number, cardholder name, expiration date) should not be retained any longer than a documented business need. The maximum period of time the data may be retained is 18 months. A regular schedule of deleting or destroying data should

be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements.

3.10 Merchant must have business recovery and continuity procedures.

3.11 Merchant must have documented data back-up processes.

3.12 MDRP must review breach procedure (3.0) with all personnel handling/processing credit cards annually.

3.13 Internal Audit, in partnership with the Ecommerce Committee, will conduct periodic testing of a random sample of merchants for compliance with this policy.

Refer to payment brand guidelines:
VISA www.visa.com/cisp
MasterCard http://www.mastercard.com/sdp/
AmericanExpress
https://www260.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US_11.pdf

4.0 Responding to a Security Breach

The University of Richmond's data exposure policy which provides action steps to follow when dealing with a security breach or suspected breach can be found at: http://is.richmond.edu/policies/general/data-exposure-policy.html

In the event of a breach or suspected breach of security, the department or unit must immediately execute each of the relevant steps below:

4.1 Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:

- Date and time
- Action taken
- Location
- Person performing action
- Person performing documentation
- All personnel involved

4.2 Contact the University of Richmond's Information Security Officer (infosec@richmond.edu) for proper direction of preservation of electronic data. The steps should include:

- Disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the computer uses a wireless connection, disconnect from the wireless network.

- DO NOT turn the computer device off or reboot. Leave the device powered on and disconnected from the network.

4.3 Notify the Dean, Director or Department Head of the unit experiencing the breach. Notify the Director of Treasury Services and Credit Card Manager.

4.4 Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on to the machine and/or change passwords; do not run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.

4.5 If a suspected or confirmed intrusion or breach of a system has occurred, the Credit Card Manager will alert the merchant bank, Internal Audit, General Counsel, University Police, the VP for Information Services and the Vice President for Business & Finance. A suspected breach may be reported to the University of Richmond by the processing bank or an outside party. In that case, the Credit Card Manager (Treasury Services) will notify the campus merchant involved in the suspected breach and the relevant steps outlined in 3.0 above should be executed.

5.0 Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected merchant. Additionally, if appropriate, any fines and assessments which may be imposed by the affected credit card company will be the responsibility of the impacted merchant.

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

6.0 Changes to this Policy

Payment card processing operates in a changing environment with changes mandated by PCI-DSS, federal and state laws and regulations. Consequently, this policy will be updated as needed.

Revision History

Version	Date Revised	Author/Editor	Comments
1	October 12, 2007	Ecommerce Committee	Initial Policy
2	March 22, 2013	Ecommerce Committee	PCI Compliant Policy