# E-COMMERCE POLICIES AND PROCEDURES FOR THE UNIVERSITY OF RICHMOND

*Last Revised: 10/12/2007*

This document governs all payment systems at the University of Richmond. The University defines a “payment system” as an application, system, process or service (electronic, manual, or paper) that allows capture, storage, authorization or access to credit cards, debit cards or electronic fund transfers (EFT). All individuals and offices that acquire or utilize a payment system provided by the University of Richmond or a third-party vendor must follow these policies and procedures. This document will evolve with Payment Card Industry (PCI) standards (https://www.pcisecuritystandards.org).

For questions or additional information about these policies and procedures, please contact the E-commerce Committee at ecommerce@richmond.edu.

## Prior to Acquiring or Utilizing a Payment System…

1) You must notify and obtain E-Commerce Committee approval prior to acquiring or utilizing a payment system for any department, organization, or individual at the University of Richmond.

2) You must include language in contracts or agreements with third-party payment systems that obligate the third-parties to comply with PCI DSS and/or PABP security standards for the duration of their relationship with the University (see below).

3) For systems hosted by an external vendor, you must provide evidence the vendor is compliant with the most recently published PCI DSS requirements and will remain so for the duration of their relationship with the University of Richmond. For more information on the definition and requirements of PCI DSS compliance, refer to https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

4) For systems hosted by the University of Richmond, you must provide evidence the application and version meets Visa’s Payment Application Best Practices (PABP): (http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html?it=l2|/merchants/risk_management/cisp.html|Payment%20Applications). In addition, you or the vendor must supply:
    - Documentation describing how the application securely transmits and stores cardholder information in all stages of processing
    - Recommended parameter settings to securely configure the payment application to meet PABP guidelines.

5) Any University department, organization, or individual that acquires or contracts with a third-party to provide a payment system that does not meet the preceding four (4) requirements, will be liable for, but not limited to, the following costs in the event of a cardholder data compromise resulting from that payment system:
   - Fines imposed by acquiring bank and/or payment brand
   - Costs to notify cardholders
   - Credit card replacement and remediation services for impacted cardholders
   - Repayment of fraudulent charges that result from data breach
   - Onsite forensics audit by a PCI-Qualified Data Security Company
   - Level 1 merchant certification by a PCI-Qualified Data Security Company

6) If required by your vendor, you must obtain deposit bank or merchant account information from the University Cash Management office.

7) You must seek E-commerce Committee approval for payment card types, fee structures, and acceptable merchant rates. Typically, you must use the following information to obtain lowest rates:
   - Cardholder name
   - Account Number
   - Expiration date
   - Billing Address
   - Phone number
   - Signature (if applicable)

## Ongoing Usage, Modification, or Upgrade of a Payment System…

1) You must notify and obtain E-Commerce Committee approval prior to upgrading or modifying a payment system.

2) If your payment process involves paper forms, you must completely destroy (shred or conceal with an indelible marker) the card validation value (CVV) and account number **immediately** after authorization.

3) If you employ student workers or floaters who have access to cardholder information, you must have them sign a Confidentiality Agreement (see Appendix B) before handling this information. Your office must maintain these forms and present them at your annual e-commerce audit.

4) You may not request, receive, or submit cardholder information via email or other insecure means.

5) You must mask cardholder account numbers on receipts, reports, and other printed documents.

6) You must physically store all paper-based cardholder information in a locked/secured location. You must not keep this information for more than 18 months (after which you must shred this information).

7) You must develop and follow written policies and procedures specific to your payment system and related processes. These policies and procedures must comply with this document. You must submit a copy of your policies/procedures to the Bursar each year during your annual e-commerce audit.

8) You are responsible for your own customer service. You must:
   - Handle all charge back disputes
   - Respond to e-commerce related customer phone calls/emails

9) You must grant and maintain non-default, unique, individual accounts for each user of your e-commerce application. The owners of these accounts must maintain secure, non-default passwords.

10) You must immediately modify/revoke the e-commerce account of any employee who changes university role or leaves the university.

11) You must not condone writing or sharing passwords.

12) You must maintain security controls dictated by PCI-DSS requirements and/or your vendor.

13) You must not store or record the card verification value (CVV) or PIN any longer than is required to process and authorize the transaction.

14) You must ensure your system/application is configured for maximum cardholder security. This includes blocking users from administrative access to the underlying system.

## Audits, Training, and Security Scans…

1) Prior to initial implementation or usage of a payment system, you must attend training facilitated by the E-commerce Committee:
   - An e-commerce workshop
   - Banner training from the Bursar and Cash Management offices

   Thereafter, on an annual basis, you must attend an annual e-commerce workshop facilitated by the E-commerce Committee. If you do not attend this workshop, the E-Commerce Committee may revoke your right to handle and process credit/debit cards and/or EFTs.

2) Prior to initial implementation or usage of a payment system, you must undergo an e-commerce audit (see Appendix A: Credit Card Audit Checklist). Thereafter, the E-Commerce Committee will audit your payment system and processes on an annual basis. If you do not pass this audit, the E-Commerce Committee may revoke your right to handle and process credit/debit cards and/or EFTs.

3) Payment systems hosted by the University of Richmond will undergo a quarterly scan by an external security vendor. If system vulnerabilities are identified by these scans, the E-Commerce Committee will work with the payment system owners to resolve or mitigate the vulnerabilities.

## Related E-commerce and PCI Resources…

**PCI Security Standards Council:**
https://www.pcisecuritystandards.org/

**Visa's Card Information Security Program (CISP):**
www.visa.com/cisp

**MasterCard Site Data Protection:**
http://www.mastercard.com/sdp/

**American Express Data Security Operating Policy:**
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home

**Educause Connect:**
http://connect.educause.edu/term_view/PCI+DSS

**PCI Forum:**
http://www.pciforum.us/pci/

**Treasury Institute (blog):**
http://www.treasuryinstitute.org/blog/

## Appendix A: Credit Card Audit Checklist
## (to be returned to Bursar’s Office)

**Audit Location:**____________________________________
**Audit Date:**_____________________
**Attendees:**___________________________________________________
____________________________________________________________

1) What credit card information is being obtained? Name, account number, expiration date, security code, billing address, phone number needed in order to get lower merchant rate.

____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________

2) Where is credit card information being stored (e.g. electronically on a university or vendor-supported system, local hard drive, reports, paper copies, etc)? All credit card numbers must be masked or encrypted on receipts, reports, or other printed documents kept at the location.

____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________

3) Are all credit card records/reports/data stored in a secure, locked location?
Who has access?

____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________

4) What credit card information are you storing and for how long?
A card holder has up to 18 months to dispute a charge.

____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________

5) Is the input on Banner being done the same day as the authorization?

____________________________________________________________
____________________________________________________________

6) Please attach specific policies and procedures for processing credit cards.  In addition to the policies/procedures developed by your office, include any documentation provided by your payment application processor or vendor.

7) Who has access to credit card information, including student workers or floaters, during all stages of processing (pre-auth, auth, reconciliation, etc)?

8) Who has access to authorize credit card transactions?

9) Who can issue credit card refunds? Who authorizes the refunds?

10) Who is responsible for following up on charge back disputes?

11) Who is responsible for training?

12) If your software, cash registers, or authorization machines require passwords how are the passwords maintained? Are they shared? Are they defaulted passwords? Explain in detail.

______________________________________________________________

______________________________________________________________

13) When an employee leaves the University, if your software, cash register, or authorization machine requires passwords, is their user name/password immediately revoked?

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

14) What security controls are in effect to prevent unauthorized individuals from gaining access to the facility where your credit card information is stored?

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

15) How is credit card information being received? (By fax, in person, over phone, web downloads, mail). No credit card information is to be requested, received or submitted via email or other unsecured channels.

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

16) Is card holder data that is printed on paper or received by fax protected against all unauthorized access? How?

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

17) a) When is sensitive credit card data destroyed?
b) When is back-up documentation destroyed?

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

18) What software and version do you use to capture, process, store, or report credit card transactions?  What is the primary vendor contact information for this system?

______________________________________________________________

______________________________________________________________

______________________________________________________________

19) Provide a copy of vendor configuration recommendations/instructions to maximize security for this system. Have these recommendations been implemented?

______________________________________________________________
______________________________________________________________
______________________________________________________________

20) If your campus-hosted system has been upgraded since the last audit, please provide a detailed data flow description illustrating how credit card information is processed and secured (encrypted) in all stages of processing, transmission, storage, and archival.

______________________________________________________________
______________________________________________________________
______________________________________________________________

____________________ ____________________ ____________________
Attendee signature Attendee signature Attendee signature

____________________ ____________________________
University Bursar Information Services

**Appendix B:** **Confidentiality Agreement**
**(to be returned to Bursar's Office)**

## University of Richmond
## Student Worker/Floater Confidentiality Agreement

**Student Employee/Floater: ____________________________**
**University ID#: ____________________**

I understand that by virtue of my employment with the University of Richmond, I will have access to records which contain individually identifiable information including credit card numbers. The disclosure of this information to anyone is prohibited. I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure also violates the University of Richmond's policy and could constitute just cause for disciplinary action including termination of employment regardless of whether criminal or civil penalties are imposed. I understand and accept these conditions of employment.

___________________ __________________________
Date Student Employee/Floater Signature

___________________ __________________________
Date UR Student Supervisor