VCU Payment Card Policy

Policy Type: Administrative  
Responsible Office: Treasury Services  
Initial Policy Approved: 12/05/2013  
Current Revision Approved: 12/05/2013

Policy Statement and Purpose

The purpose of this policy is to help ensure that VCU is (1), being a good steward of personal cardholder information entrusted to it by its students, parents, donors, alumni, customers and any individual or entity that utilizes a credit card to transact business with the university, (2), complying with the Payment Card Industry Data Security Standards (PCI DSS) and (3), striving to prevent unauthorized and inappropriate use of cardholders’ information.

VCU is committed to complying with the PCI DSS by ensuring the secure handling of payment card information. All university merchants accepting payment cards are required to comply with the PCI DSS and this policy for accepting and handling payment card transactions.

Treasury Services and Technology Services have been assigned responsibility for assessing, determining, and monitoring compliance with these standards. As a result, responsibility for determining how to apply these standards and for assessing deficiencies is shared among these named areas. Treasury Services will provide direction and assistance on business processes related to card operations and Technology Services will provide direction and assist with technical implementation and security issues.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who Should Know This Policy</td>
<td>2</td>
</tr>
<tr>
<td>Definitions</td>
<td>2</td>
</tr>
<tr>
<td>Contacts</td>
<td>2</td>
</tr>
<tr>
<td>Procedures</td>
<td>3</td>
</tr>
<tr>
<td>Forms</td>
<td>5</td>
</tr>
<tr>
<td>Related Documents</td>
<td>5</td>
</tr>
<tr>
<td>Revision History</td>
<td>5</td>
</tr>
<tr>
<td>FAQs</td>
<td>6</td>
</tr>
</tbody>
</table>
**Who Should Know This Policy**

VCU faculty, staff, students, contractors and third party vendors that collect, maintain or have access to payment card information are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

**Definitions**

**Approved Scanning Vendor**
An Approved Scanning Vendor (ASV) is an organization that validates adherence to certain PCI-DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers. The PCI council has approved over 130 ASVs.

**Cardholder Data**
The Primary Account Number (PAN) alone or the PAN plus any of the following: full magnetic stripe information, cardholder name, service code or expiration date.

**Merchant**
Any entity that accepts payment cards as payment for goods and/or services.

**Merchant Account**
A relationship set up by Treasury Services through the bank and a credit card processor in order to process payment cards as payment for goods or services rendered by the account holder. The merchant account is tied to a Banner index to distribute funds appropriately to the merchant (owner) for which the account was set up.

**Payment Card**
Credit cards, debit cards or charge cards issued by a financial institution.

**PCI-DSS**
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to alleviate vulnerabilities that put cardholder data at risk.

**Service Provider**
Any company that stores, processes or transmits cardholder data on behalf of another entity is defined to be a service Provider by the Payment Card Industry (PCI) guidelines.

**Third Party Processor**
A company that offers Payment Card processing software and/or gateway services. All Third Party Processors must be PCI DSS Compliant in order for a department to obtain or maintain a merchant account.

**Contacts**

Treasury Services and Technology Services are responsible for this policy. Treasury Services is responsible for obtaining approval for any revisions as required by the policy *Creating and Maintaining*
Policies and Procedures through the appropriate governance structures. Please direct policy questions to Treasury Services. Technical security questions should be directed to Technology Services.

Procedures

University departments must request and receive approval from Treasury Services prior to accepting payment cards. Treasury Services will assist departments in establishing processes and appropriate controls through on-line training. *All university departments that process payment card transactions for goods and services are deemed to be merchants under the PCI DSS*.

Third party vendors (processors, software providers, payment gateways, or other goods or service providers) who accept credit card transactions on behalf of the University must contractually agree to: (1) adhere to all applicable requirements in PCI DSS, (2) be liable for the security of the cardholder data, (3) notify the University of any breaches or intrusions within 72 hours of discovery, and (4) periodic information security reviews by the University. Detailed procedural steps are provided below to ensure full compliance.

1. **Compliance with PCI DSS Standards**
   Departments accepting payment cards are expected to adhere to these standards which are updated periodically and to verify the compliance of third party service providers. The standards can be summarized as follows:
   - Build and Maintain a Secure Network
   - Protect Cardholder data
   - Maintain a Vulnerability Management Program
   - Implement Strong Access Control Measures
   - Regularly Monitor and Test Networks
   - Maintain an Information Security Policy

   The university prohibits electronic storage of cardholder data because of the additional risks associated with protecting the stored data. Requirements apply to departments that collect card information in any format for processing. Paper records containing payment card information must be destroyed in accordance with the PCI DSS and Library of Virginia’s Record Retention Schedule.

   Departments shall agree to forward necessary system and network log information from its payment card systems and associated network devices to security monitoring tools managed by Technology Services for detection and prevention of threats targeting these systems. Departments shall also agree to allow periodic security scans and testing of its payment card systems by both Technology Services and selected Approved Scanning Vendor. Further, if applicable, with guidance from Treasury Services and Technology Services, departments are responsible for the completion of an annual Self-Assessment Questionnaire (SAQ) as required by PCI DSS.

2. **Payment Card Acceptance**
Any entity that accepts payment cards as payment for goods and/or services is a merchant. Once merchant accounts are enabled for a department, the department has an ongoing responsibility to understand security requirements, comply with PCI DSS standards, and to maintain proper business practices as described further in various procedures and guidelines associated with this policy.

Annually, individuals must be trained in the proper handling of payment card information and must complete the Responsibilities of Credit Card Handlers and Processors form. Access to payment card data by university employees must be limited to those individuals with a business need.

Employees must have a unique login identification and password to access computer systems or programs that contain payment card information to ensure individual accountability. Vendor-supplied defaults for system passwords and other security parameters are not to be used.

Departments are responsible for paying all fees and other costs associated with accepting payment cards including equipment and technology costs, banking fees, and external security assessment fees as required by PCI DSS.

3. **Use of Third Party Software**
   Only University approved compliant e-commerce applications may be used. Departments whose needs cannot be met due to the list of pre-approved software applications that are PCI DSS compliant must request prior approval from Treasury Services and Technology Services before considering or acquiring third party solutions. Third party processors must provide proof of PCI DSS compliance on an annual basis to Treasury Services.

4. **Secure Transmissions**
   To ensure that proper business practices and security are maintained, only secure and approved processes are conducted through approved web vendors, analog telephone lines for point of sale terminals and/or PCI compliant IP credit card terminals. Any unapproved processes, including email, are not allowed to transmit or store payment card information.

5. **Security Breaches**
   All known or suspected security breaches of cardholder information must be reported immediately to the department head, Treasury Services at 828-6533 and the Technology Services Information Security Office via the VCU Help Desk at 828-2227. Departments must cooperate fully with any resulting investigation.

6. **Sanctions for Non-Compliance**
   University departments that transact business using payment cards in a manner that deviates from this policy are subject to various financial and other sanctions. These may include termination of merchant accounts, financial penalties and costs associated with a security breach, penalties and costs associated with bringing a non-compliant application into compliance, and/or possible disciplinary action of the individual involved – up to and including termination of employment.
**Forms**

1. Responsibilities of Credit Card Handlers  
   (http://www.vcu.edu/treasury/CCResponsibilities.pdf)

2. Request for a New Merchant Account (Jessica has this form, and it is not a live URL yet, but she has given me the form)

**Related Documents**

1. Payment Card Industry Data Security Standard  
   (https://www.pcisecuritystandards.org/)

2. Credit Card Merchant Accounts  
   (http://www.vcu.edu/treasury/CreditCardMerchantAccount.htm)

3. University Cash Receipting Policies and Procedures  
   (http://www.vcu.edu/treasury/CashieringOperationsGuidelines.htm)


5. Records Management (http://ts.vcu.edu/askit/1947.html)

6. Computer and Network Resources Use Policy  
   (http://www.ts.vcu.edu/askit/3409.html)

**Revision History**

None – New Policy

**FAQs**

1. To whom does PCI apply?
   
   PCI applies to all university departments that accept, transmit or store any cardholder data regardless of size or number of transactions.

2. Who set the standards?
   
   The standards are set by the PCI Security Standards Council. The PCI Council was created in 2006 to align the separate security programs and standards of major card programs; American Express, Discover Financial Services, JCB, MasterCard Worldwide and VISA International.

3. What constitutes a payment application?
   
   A payment application is anything that stores, processes or transmits card data electronically. This means that anything from a Point of Sale System (swipe terminals) to a web e-commerce site are
all classified as payment applications. Any piece of software that has been designed to touch payment card data is considered a payment application.

4. What are the costs of non-compliance with PCI DSS?

The cost of non-compliance will result primarily from a security breach if cardholder information is compromised. These costs may include:

- Notifying affected cardholders
- Paying for credit monitoring for the affected parties
- Paying for unauthorized charges
- Implementing needed hardware or software upgrades to comply with a higher level of security that would be required post-breach
- Fines from credit card companies and PCI council
- Litigation from cardholders, vendors or credit card companies
- Unfavorable publicity
- Damage to VCU’s reputation
- Temporary or permanent loss of ability to process payment cards

5. How do payment card security breaches happen?

Types of Breaches:

- Hacking into networked computers
- Loss of stolen PCs, Media
- Improper disposal of records (paper records not shredded or properly disposed)
- Intentional disclosure or fraud
- Unintentional disclosure due to human error

Sources of Breaches:

- Improper storage of data
- Insecure applications
- Inadequate network security controls
- Unpatched systems and/or default configuration
- Insecure wireless access points
- Use of default passwords
- No intrusion monitoring
- Unsecured point of sale technology
- Malicious Insider