Payment Card Compliance

Policy Type: Administrative
Responsible Office: Treasury Services, Office of the Vice President for Finance and Budget
Initial Policy Approved: 12/05/2013
Current Revision Approved: 02/20/2017

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 are responsible for assessing, determining, and monitoring compliance with these standards. Responsibility for determining how to apply these standards and for assessing deficiencies is shared among Treasury Services and Technology Services. Treasury Services provides direction and assistance on business processes related to card operations and Technology Services provides direction and assists 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

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 (ASV)
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 strip information, cardholder name, service code or expiration date.

Payment Card Merchant (“Merchant”)
Any entity that accepts payment cards as payment for goods and/or services.

Payment Card Merchant Account (“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 payment card 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.

Payment Card Industry Data Security Standard (PCI DSS)
Payment Card Industry Data Security Standard (PCI DSS) 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 the deputy treasurer in Treasury Services. Technical security questions should be directed to the information security officer in Technology Services.

Policy Specifics and Procedures

All university departments that process payment card transactions for goods and services are deemed to be merchants under the PCI DSS. Such 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 to comply with this policy through on-line training.

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 Technology Services. Detailed procedural steps are provided below to ensure full compliance.

1. **<u>Compliance with PCI DSS Standards</u>**
   Departments accepting payment cards must adhere to these standards which are updated periodically and verify the compliance of third party service providers annually. The standards can be summarized as follows:

   - Build and Maintain a Secure Network
     - Install and maintain a firewall configuration to protect cardholder data
     - Do not use vendor-supplied defaults for system passwords and other security parameters
   - Protect Cardholder Data
     - Protect stored cardholder data
     - Encrypt transmission of cardholder data across open, public networks
   - Maintain a Vulnerability Management Program
     - Protect all systems against malware and regularly update anti-virus software or programs
     - Develop and maintain secure systems and applications
   - Implement Strong Access Control Measures
     - Restrict access to cardholder data by business need to know
     - Identify and authenticate access to system components

        - Restrict physical access to cardholder data
  - Regularly Monitor and Test Networks
    - Track and monitor all access to network resources and cardholder data
    - Regularly test security systems and processes
  - Maintain an Information Security Policy
    - Maintain a policy that addresses information security for all personnel

The university prohibits electronic storage of cardholder data because of the additional risks associated with protecting the stored data. This requirement applies 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 must forward upon request 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 must also allow periodic security scans and testing of its payment card systems by both Technology Services and selected approved scanning vendor upon request. Further, upon notification by and with guidance from Treasury Services and Technology Services, certain departments are responsible for the completion of an annual Self-Assessment Questionnaire (SAQ) as required by PCI DSS.

2. <u>Payment Card Acceptance</u>

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 listed in the Related Documents section below.

Annually, individuals responsible for or involved with credit card processing 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. <u>Receiving and Depositing Credit Cards</u>

University departments are permitted to accept VISA, Master Card, Discover and American Express for payments, provided that prior approval is obtained from the Treasury Reporting office within Treasury Services. Payments made by credit cards must be recorded on sales slips or printed on single-ply paper. Designated departments must process credit card payments and credits on point-of-sale terminals that print the transacting information on single-ply paper. It is strongly suggested that charges and credits include the customer's telephone number. Credit cards should be verified to a driver's license or other acceptable proof of identification. If a refund is necessary for a customer that paid by credit card, a credit must be made to the credit card. Cash or check refunds are not permissible in accordance with credit card regulations. The total amount of the credit card transaction is subtracted from the amount of the total sales to obtain net sales.

At the end of each business day, the net sales (or credit) for the day must be transmitted to the bank card center by closing the batch on the point-of-sale terminal. The batch total must agree to the net sales for the day.

Departments using cash registers must record all credit cards sales on the cash register and the appropriate entries must be recorded in Banner.

All deposits must be reconciled with the sales slips, and the register tapes, if applicable. The deposits must be traced to the appropriate index in Banner.

4. **Payment Card Charge Backs**
A charge back occurs whenever a card error or discrepancy is observed by the cardholder. The bank card center charges back the university's bank and notifies Treasury Reporting. Upon receipt of the charge back, Treasury Reporting will debit the department's index of original deposit. The department must provide Treasury Reporting with a copy of the sales slip. Treasury Reporting will notify the bank card center of the department's proof of charge. If the bank card center reverses the charge back, the department's index will be credited.

5. **Use of Third Party Software**
Only university approved compliant e-commerce applications are permitted to 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.

6. **Secure Transmissions**
To ensure that proper business practices and security are maintained, only secure and approved processes verified by Treasury Services and Technology Services are permitted to be conducted through approved web vendors, analog telephone lines for point of sale terminals and/or PCI compliant IP credit card terminals. IP enabled devices designed to transmit credit card information must be placed on a PCI network dedicated for the transmission of credit card information. Any unapproved processes, including email, are not permitted to transmit or store payment card information.

7. **Security Breaches**
All known or suspected security breaches of cardholder information must be reported immediately to the department head, Treasury Services at 804-828-6533 and the Technology Services Information Security Office via the VCU Help Desk at 804-828-2227. Departments must cooperate fully with any resulting investigation.

8. **Sanctions for Non-Compliance**
University departments are prohibited from transacting business in a manner that deviates from this policy. University departments that deviate 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 and Processors
2. Request for a New Merchant Account

Related Documents

1. Payment Card Industry Data Security Standard (https://www.pcisecuritystandards.org/)
2. Payment Card Industry Compliance Training
3. VCU Policy*: Information Security*
4. Records Management
5. VCU Policy: *Computer and Network Resources Use*
6. Credit Card Merchant Accounts

Revision History

December 05, 2013	*VCU Payment Card Policy*
August 25, 2017	*Payment Card Compliance* [minor revision to include the “Receiving and Depositing Credit Cards” and “Payment Card Charge Backs” sections from the *Treasury Services Policies and Procedures* policy, which has been retired]

FAQ

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

6. What should I do if my department would like to take credit card payments?

Contact VCU Treasury Services at 804-827-1876 for guidance on the setup of your environment dedicated to take card payments. At a minimum, the department will need to:

- Register with VCU Treasury Services
- Obtain Merchant ID from VCU Treasury Services
- Obtain approved terminals for card processing
- If third party or IP based terminals are used, work with VCU Technology Services on configuration of secure network