Accepting and Handling Payment Card Transactions

No. 3610

Policy Effective Date:
12/14/2011

Last Revision Date:

Policy Owner:
Dwight Shelton

Policy Author:
(Contact Person)
Savita Sharma

Affected Parties:
Faculty
Staff

1.0 Purpose

The purpose of this policy and related university procedures is to ensure that credit and debit card information, hereafter referred to as payment card information, is accepted and handled securely to reduce the risk of identity theft and financial fraud to university customers who make payments via such methods.

To reduce their losses due to credit card fraud, five members of the payment card industry, Visa, Inc., MasterCard Worldwide, American Express, Discover Financial Services, and JCB International (Japan Credit Bureau), banded together to develop security standards for any organization that accepts, captures, stores, transmits, and/or processes payment card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry's Data Security Standard, or PCI DSS (https://www.pcisecuritystandards.org/). The PCI DSS is an evolving set of comprehensive requirements designed to enhance payment account data security. The PCI DSS contains six categories of requirements. These include building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

Virginia Polytechnic Institute and State University, hereafter referred to as the university, 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. Additional procedures, announcements, and training opportunities are published on the Bursar's website (www.bursar.vt.edu).

This policy and university procedures are designed to be in compliance with PCI DSS and help university merchants that process payment card transactions proactively protect payment card data. Non-compliance with the standard can result in the compromise of payment card data and in turn have far reaching consequences for the university, including regulatory notification requirements, loss of reputation, loss of customers, potential significant financial liabilities (for example, regulatory and other fees and fines), and litigation.

2.0 Policy

University entities must request and receive approval from the Office of the University Bursar to accept payment cards. Only entities that have established processes and appropriate controls in place will be approved to accept payment cards for goods and services. All university entities that process payment card transactions for goods and services are deemed to be merchants under the PCI DSS. Existing university merchants who process or transmit payment card data, as well as any new entity that desires to accept payment cards for good or services, must adhere to this policy and university procedures, ensuring compliance with the PCI DSS.

University merchants that capture, process, store, or transmit payment cards in exchange for goods and services must adhere to the following:

1. PCI DSS compliance is mandatory for any university merchant that accepts, captures, stores, transmits, and/or processes payment card information. This policy and university procedures have been designed to ensure compliance with the standards.
2. Only authorized and properly trained university merchants and employees may accept, process, and/or access payment card information.
3. University merchants must develop and maintain administrative and information technology security procedures related to their payment card operations that are in compliance with this policy and university procedures.
4. Payment cards may be accepted only using methods approved by the Office of the University Bursar. New technology evolutions must be approved prior to implementation and must be properly secured and documented. Procurement of any software applications, third party services, or development of payment channels must be approved by the University Bursar prior to execution of contractual agreements.
5. Every individual who has access to payment card information is responsible for protecting the information.
6. All types of media containing payment card information must be retained and destroyed in accordance with the PCI DSS, Library of Virginia's Record Retention Schedule (www.lva.virginia.gov/records/retention) and the University's Best Practices for Handling Payment Cards, located on the bursar's website at www.bursar.vt.edu/paymentcard.
7. All employees of the university who are involved in the accepting, processing, or reconciling of payment card sale transactions are required to complete Payment Card Training and a Payment Card Security Agreement annually.
8. University merchants must annually validate compliance of the payment card requirements (via a method approved by the PCI Security Standards Council). The University Payment Card Coordinator will coordinate the annual validation with all university merchants.
9. Suspected exposure or theft of payment card information must be reported immediately to the University Payment Card Coordinator in the Bursar's Office. University merchants suspecting criminal activity should immediately contact the Virginia Tech Police Department and the Payment Card Coordinator.

University merchants accepting cards using methods other than the university's preferred hosted payment solution or stand alone, dial-out phone terminals must comply with requirements of the PCI DSS in addition to those above based on the method of card acceptance. The university may require its merchants to have an independent Qualified Security Assessor (as defined by the PCI DSS) to review and assess payment card activities and documentation and affirm the annual validation of compliance of the payment card requirements.

University merchants accepting payment cards are responsible for all costs of compliance with the PCI DSS including scanning, penetration testing, network infrastructure changes, and external assessments. Further, entities are responsible for any financial penalties assessed by the bank(s) or brand(s) in the event of data breach or failure to maintain compliance with the PCI DSS.

The University Payment Card Coordinator will coordinate and direct the annual validation process and required quarterly scans, conduct periodic onsite reviews of all university merchants, and recommend self-assessment or external assessment of each university merchant. University merchants failing to comply with the principles above may lose their authorization to process payment card transactions, and individuals failing to accept and process payment cards in accordance with university and departmental policies and procedures may be subject to disciplinary action and termination in addition to criminal and civil penalties imposed by law.

3.0 Procedures

The procedures below are in support of the policy principles listed above.

1. **PCI DSS compliance is mandatory for any university merchant that accepts, captures, stores, transmits, and/or processes payment card information. This policy and university procedures have been designed to ensure compliance with the standards.**

   Any university merchant that accepts payment cards must handle payment card information securely by following this policy along with university and departmental procedures. 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.

2. **Only authorized and properly trained university merchants and employees may accept, process, and/or access payment card information.**

   Any university entity desiring to accept payment cards must notify and obtain prior written approval from the Office of the University Bursar before acquiring, contracting or utilizing a payment card system. University merchants are responsible for all expenses associated with payment card merchant accounts, including but not limited to equipment costs and banking fees. University merchants may not adjust the prices of goods and services based upon the method of payment or directly pass along any fees associated with accepting payment cards to the customer. The contractual terms of the agreements that the university has with the credit card companies does not permit different price structures based on payment type. University merchants are, however, encouraged to work with the Office of Budget and Financial Planning to establish a pricing structure based on the total cost of doing business.

   University merchants must provide in writing to the Office of the University Bursar requests to change the method by which they accept or process payment cards, including the purchase, lease or replacement of any equipment or system utilized to accept and process payment cards. Notice must be given to the Office of the University Bursar for any request by a university merchant to terminate their merchant identification number and cease accepting payment cards for goods and services.

3. **University merchants must develop and maintain administrative and information technology security procedures related to their payment card operations that are in compliance with the PCI DSS. This policy and university procedures are designed to ensure university departments accepting payment cards are in compliance with the PCI DSS.**

   Each university merchant that handles payment card information must have written procedures specific to its operations that are consistent with this policy and other related university policies and procedures such as Information Technology Security, Funds Handling, and Fiscal Responsibility. The procedures should include, but not be limited to: segregation of duties, deposits, reconciliation procedures, physical security and identification of card processing area, disposal, storage, separate passwords, firewall, anti-virus software, cash

register procedures and personnel screening and criminal conviction check procedures. See University Policy 4060, Conviction and Driving Record Investigation for Employment (http://policies.vt.edu/4060.pdf).

When an employee is no longer involved with payment card operations due to termination or a change in job responsibilities, access to payment card information, keys, access codes, and passwords must be revoked and/or changed immediately to prevent any future unauthorized access.

University merchants handling payment card transactions must segregate all duties related to data processing and storing of payment card information. For example, the same person that processes payment card transactions cannot perform the monthly reconciliation or process refunds.

The manual or electronic collection of the full sixteen digit cardholder number, referred to as the primary account number (PAN), is discouraged. All paper based processes where customers write down their payment card number and provide it to a university merchant should be re-engineered to utilize the university's preferred hosted payment solution or point of sale, stand-alone dial out phone terminals. Any paper media containing the full sixteen digit cardholder number must be kept in a locked and secured location at all times and destroyed after authorization of the transaction. All point of sale swipe payment card machines must mask the payment card number on both the merchant and customer copies of the receipt and any batch and settlement report(s). When utilizing the university's preferred hosted payment solution, the customer enters their payment card number on an externally hosted website for processing, eliminating the need for university employees to collect their payment card number.

Verification of controls and approval of University Bursar must be obtained prior to storage of any *cardholder data* and annually thereafter. Electronic storage of *Sensitive Authentication Data* and unencrypted *cardholder data* is prohibited. This includes but is not limited to any computer program, university system, email, or any electronic visual image.

In addition to the PCI DSS, university merchants must comply with the Standard for Storing and Transmitting Personally Identifying Information, which is located on the Information Technology Security Officer's website.

4. Payment cards may be accepted only using methods approved by the Office of the University Bursar.

All university merchants who accept card payments via the internet are required to use the university's preferred hosted payment solution. Stand alone, dial out phone terminals are the preferred method for in-person acceptance of card payments. University merchants considering changes to collection of card data, such as kiosks, telephone orders, call centers operations, etc. with higher risks must update their merchant ID application with the Bursar's office and receive approval prior to implementation. See Exceptions section of this policy for guidance on the approval of other processing methods.

New technology evolutions must be approved prior to implementation and must be properly secured and documented. Procurement of any software applications, third party services, or development of payment channels for the acceptance of credit cards must be approved by the University Bursar prior to execution of contractual agreements.

All university contracts with a third party organization to accept, store, and/or process payment card information on the university's behalf must have contract language requiring the third party's compliance with PCI DSS. The university merchant shall be responsible for obtaining written notice of compliance on an annual basis and forwarding it to the University Payment Card Coordinator.

5. **Every individual who has access to payment card information is responsible for protecting the information**.

   Individuals must be trained in the proper handling of payment card information. Individuals who are new to the role must be trained prior to assuming their payment card handling duties. Access to payment card data by university employees must be limited to those individuals with a business need.

   University employees are prohibited from intentionally disclosing sensitive payment card information to any unauthorized person and may be subject to criminal and civil penalties imposed by law, including disciplinary action and termination.

   Protected payment card information including PAN, cardholder name, service code, expiration date, and any sensitive authentication data must not be requested, received, or transmitted through an unsecure medium. End user messaging technologies such as email, text or instant messaging (encrypted or unencrypted) are not acceptable methods for receiving credit card information. University merchants are prohibited from accepting credit card information via end user messaging technologies. Each university merchant's card handling procedures must include documented procedures for handling transactions received through unsolicited channels that prescribe said approved channels and prohibit processing card information received via end user messaging technologies.

   University merchants are responsible for any monetary sanctions and/or card acceptance restrictions imposed as a result of a payment card data compromise if the unauthorized disclosure of cardholder data is due to their direct negligence or failure to adhere to this policy or university procedures.

   All employees who have payment card responsibilities must be screened for security risks including a criminal conviction check indicating no convictions of financial fraud or related illegal activities before being assigned responsibilities for accepting, processing, or accessing sensitive payment card information. University merchants may contact the Office of the University Bursar in writing to request an exception to this procedure in cases where the entity has individuals that are tasked with accepting and immediately processing over-the-counter card transactions, but have no access to lists, reports, or storage areas where card information is held.

   Employees must have a unique login identification and password to access computer systems or computer programs that contain payment card information to ensure individual accountability and segregation of duties. The sharing of passwords or log-in information is strictly prohibited. Each individual employee is responsible for keeping their login identification and password confidential.

6. **Payment card information must be retained and destroyed in accordance with PCI DSS, Library of Virginia's Record Retention Schedule, and Best Practices, located on the bursar's website.**

   University merchants must have procedures in place to comply with the more stringent requirements of the PCI DSS for the collection and destruction of cardholder data. The creation of paper media containing *cardholder data* is discouraged and should be kept to a minimum. If there is a business need to collect the PAN, once the business need no longer exists, the university merchant must cross-cut shred, pulp or incinerate the PAN in accordance with PCI DSS.

   Other paper records (i.e. paper payment card receipts) related to payment transactions such as day end reports for balancing and specifically not including defined *cardholder data* must be securely stored and retained in accordance with the Library of Virginia's Record Retention Schedule. Once the records are ready for destruction, university merchants must ensure that records are destroyed in accordance with the PCI DSS and University Policy 2000, Management of University Records (http://policies.vt.edu/2000.pdf).

7. **All employees of university merchants who are involved in accepting, processing, or reconciling of payment card sale transactions are required to complete Payment Card Training and a Payment Card Security Agreement annually.**

   Upon hire and at least annually, all employees who are involved with the acceptance, processing or reconciling of payment card transactions are required to complete Payment Card Training offered by the university and complete a Payment Card Security Agreement, confirming their understanding and adherence to this policy. University merchants must maintain records of employees' training.

8. **University merchants must complete an annual assessment (through a method approved by the PCI Security Standards Council) to validate and document compliance with the payment card requirements. The University Payment Card Coordinator will coordinate the completion of the annual assessment with all university merchants.**

   Annually, university merchants are required to validate compliance with the PCI DSS. This effort will be coordinated by the University Payment Card Coordinator with the assistance of the Information Technology Security Office. The Payment Card Coordinator will provide assistance on business processes related to card operations and the Information Technology Security office will assist with technical security issues.

   University merchants are subject to review and audit of compliance with payment card policies on a recurring basis (by the Bursar Office, internal and external auditors), as well as a review of technical security by the Information Technology Security Office. Any vulnerability identified via audit or areas of non-compliance with the PCI DSS must be resolved promptly. The Office of the University Bursar reserves the right to temporarily suspend or terminate a university merchant's authorization to accept payment cards for non-compliance.

9. **Suspected exposure or theft of payment card information must be reported immediately to the University Payment Card Coordinator in the Bursar's Office. University merchants suspecting criminal activity should immediately contact the Virginia Tech Police Department and the Payment Card Coordinator.**

   In the event of an unauthorized disclosure of payment card data, which includes the suspected unauthorized access of electronic data or paper media, the university merchant should immediately contact the University Payment Card Coordinator. If criminal activity is suspected the Virginia Tech Police Department should be the first point of contact. Once an incident has been validated and any potential exposure verified, procedures for contacting individuals will be determined by university administration, university legal counsel, and outside entities, as required by contract or law.

4.0 Exceptions

Written authorization must be obtained from the University Bursar for any university merchant or entity seeking an exception to any portion of this policy. University merchants seeking exception must submit a written request identifying the business need and the measures proposed to ensure compliance with the PCI DSS. It is recommended that university merchants perform a detailed review of business processes and costbenefit analysis, considering all processing channels that may be of lower risks or costs. Request(s) must at a minimum include the following:

a. Identification and position description of the employee(s) charged with full PCI DSS compliance
b. Description of business need for collection or storing of cardholder data
c. Software applications and validation of PCI DSS compliance, including copy of contracts
d. Incident response plans
e. Data Retention and disposal procedures
f. Network diagram(s)

5.0 Definitions

The following is a summary of terms used and defined in this policy.

ASV – Approved Scanning Vendors are organizations that validate adherence to the PCI DSS by performing remote vulnerability scans of internet facing environments.

Cardholder/Payment card data - the Primary Account Number (PAN) alone or the PAN plus any of the following: cardholder name, expiration date, or service code – encoded number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction.

Cardholder data environment – the people, processes and technology that store, process or transmit cardholder data or sensitive authentication data including any connected system components.

Compromise also referred to as "data compromise" or "data breach" - intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.

IP (Internet protocol) - network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.

Merchant – a university entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Merchant employees – full-time, part-time, temporary or student employees of the university whose job responsibilities include the handling of payment cards or payment card records containing cardholder data on behalf of the entity's merchant account.

PAN – primary account number is the fifteen or sixteen digit payment card number on the front of the card that identifies the issuer and the particular cardholder account.

Payment Card – a credit or debit card issued through one of the five members of the payment card industry – Visa, Master Card, American Express, Discover, or JCP.

PCI DSS – Payment Card Industry Data Security Standard, a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Preferred Hosted Payment Solution - hosted payment processing solution managed by the bursar's office that provides a common platform for online payments meeting the requirements of PCI DSS. The preferred hosted payment solution may be stand-alone or integrated with ordering and receivable systems.

Self-Assessment Questionnaire (SAQ) – a validation tool to assist merchants in self-evaluation of compliance with the PCI DSS.

Sensitive Authentication Data – security related information (including but not limited to full magnetic stripe data, card validation value/code (CAV2/CVC2/CVV2/CID) and personal identification number (PINs/PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

University Payment Card Coordinator – the individual assigned the responsibility by the University Bursar for the oversight and management of the university's payment card program to ensure compliance with PCI DSS standards.

6.0 References

The following policies and guidelines supplement and help to create a comprehensive credit card security plan. Referral and adherence to these documents is imperative to the overall protection of sensitive payment card information. The following policies and laws are incorporated by reference into this policy:

Policy 1040, Reporting and Investigating Suspected Fraudulent Activities
www.policies.vt.edu/1040.pdf

Policy 2000, Management of University Records
www.policies.vt.edu/2000.pdf

Policy 3600, Funds Handling and Deposit of State and Local Funds
www.policies.vt.edu/3600.pdf

Policy 4060, Conviction and Driving Record Investigation for Employment
www.policies.vt.edu/4060.pdf

Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
www.policies.vt.edu/7000.pdf

Policy 7010, Securing Technology Resources and Services
www.policies.vt.edu/7010.pdf

Policy 7025, Safeguarding Nonpublic Customer Information
www.policies.vt.edu/7025.pdf

Policy 7100, Administrative Data Management and Access Policy
www.policies.vt.edu/7100.pdf

Library of Virginia's Record Retention Schedule
http://www.lva.virginia.gov/agencies/records/retention.asp

Standard for Storing and Transmitting Personally Identifying Information
http://www.it.vt.edu/content/dam/it_vt_edu/policies/PII_October2011_Rev_1.pdf

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

7.0 Approval and Revisions

Approved December 14, 2011 by Vice President for Finance and Chief Financial Officer, M. Dwight Shelton, Jr.