VH | Virginia Highlands
COMMUNITY COLLEGE

VHCC Policy for Accepting and Handling Credit and Debit Card Payments

Purpose

This document describes Virginia Highlands Community College’s policy and procedures for the proper handling of credit and debit card transactions processed through automated systems and/or manual procedures. It is intended for:

- Any individual who accepts, captures, stores, transmits and/or processes of credit or debit card payments received for the purchase of College products and services, for contributions, etc.

- Any individual who supports any College effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives him or her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, etc.

This policy and procedures are intended to ensure that credit and debit card information is handled and disposed of in a manner that satisfies the College’s obligation to protect such information to the level that meets or exceeds that required by the Payment Card Industry.
Since any unauthorized exposure of credit or debit card information could subject the College to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter.

Background

To reduce their losses due to credit card fraud, five members of the payment card industry, Visa, Master Card, American Express, Discover and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit 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.” PCI-DSS is enforced through the contracts that Virginia Highlands Community College, as a merchant account holder, has with our merchant bank, i.e., the financial institution that serves as a liaison between Virginia Highlands Community College merchants and the payment card companies. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.
For additional information about PCI-DSS, please visit the Payment Card Industry’s Web site at: https://www.pcisecuritystandards.org. College Policy and Procedures for Accepting and Handling Credit and Debit Card Payments.

Principles

Virginia Highlands Community College is committed to complying fully with the expectations specified by the Payment Card Industry in its Data Security Standard (PCI-DSS). Compliance by Princeton requires that:

1. PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information.

2. Only authorized and properly trained individuals may accept and/or access credit or debit card information.

3. Credit and debit card payments may be accepted only using methods approved by the College IT Security Officer and the College Finance Manager.

4. Each person who has access to credit or debit card information is responsible for protecting the information.

5. Credit and debit card information must be destroyed as soon as it is no longer necessary.

6. Departments must maintain appropriate checks and balances in the handling of credit and debit card information

7. Each department that handles credit and/or debit card information must have documented procedures for complying with this policy and PCI-DSS.

8. Suspected theft of credit or debit card information must be reported immediately to the College IT Security, Finance Manager and Campus Police Chief.

Failure to comply with these principles, as implemented in this Policy, may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action.
The following section defines the College’s standard procedures in support of the above principles.

Procedures to Implement the College’s Credit and Debit Card Principles

1. PCI-DSS Compliance is Mandatory for any Department that Accepts, Captures, Stores, Transmits and/or Processes Credit or Debit Card Information.

Any College department that accepts credit or debit cards as payment for goods and/or services must comply with PCI-DSS to ensure the security of cardholder information. Compliance with the requirements of this policy (as updated or amended) satisfies the elements of compliance with PCI-DSS.

2. Only Authorized and Properly Trained Individuals May Accept and/or Access Credit or Debit Card Information

No individual is authorized to accept, access or support systems housing credit or debit card information until the following requirements are satisfied:

- The individual must be authorized by their appropriate Academic or Administrative Department Manager, Dean or Director to do so.

- The individual must be trained in the proper handling of credit and debit card information. Individuals who are new to the role must be trained prior to taking on their credit or debit card handling duties. Individuals whose credit or debit card handling responsibilities preceded the implementation of this policy should receive training as soon as possible.

- The individual must acknowledge his or her understanding of this policy and must confirm his or her commitment to comply with all related College policies and procedures before he or she assumes credit and/or debit card handling duties and on an annual basis thereafter. This requirement may be satisfied by completion of the annual SANS Training.

- In cases where the individual is tasked with taking and immediately processing over-the-counter or over-the-phone credit or debit card transactions, but has no access to lists, reports and/or storage areas where credit or debit card information is held, a criminal background check and credit check is recommended but is not mandatory.

- No individual is authorized to access any lists, reports and/or storage areas where credit or debit card information is stored in electronic, magnetic, optical and/or physical (e.g., paper) form, or to support computer systems that store or process credit or debit card information until the following additional requirements are satisfied:
  - The individual must be an employee of the College.

  - The appropriate Academic or Administrative Department Manager, Dean or Director must request that the Human Resources Department perform a criminal background check and a credit check on any prospective employee who may have access to such data. A credit and criminal background check also must be performed for prospective technical support personnel who have access to any computer system or application program that accepts, captures, stores, transmits or processes credit or debit card information.

  - In cases where either check returns outstanding issues, the appropriate Department Manager, Dean or Director will review those issues with Human Resources and the Office of the General Counsel to determine whether or not the individual should be permitted to handle credit card information.

  - The appropriate Academic or Administrative Department Manager, Dean or Director must provide the Human Resources Department with a list of positions that require background checks, and must ensure that the job description for any position that requires a background check will indicate that such a check will be performed.

3. Credit and Debit Card Payments May Be Accepted Only using Methods Approved by the College IT Security Officer and the College Business Office Manager Office

Credit and debit card payments may only be accepted in the following manner:

- in person

- via telephone,

- via FAX,

- through a PCI-DSS-compliant automated system that is entirely hosted by a PCI-DSS-compliant third party organization approved by the Virginia Community College System Office,

- through an automated system that is hosted in the Virginia Community College's data center that does not accept, capture, store, transmit or process credit or debit card information itself, but refers the customer to a PCI-DSS-compliant system hosted by a third party organization, approved by the Virginia Community College System Office, which handles credit and debit card payments on our behalf. The third party system must not return credit card numbers, expiration dates or verification values to the College-based system.

Any department that uses a third party organization to accept, store and/or process credit or debit card information on its behalf, except for any third-party organization that already has a campus-wide agreement with the College Business Office Manager, must receive from the vendor, on an annual basis, and keep on file documentation indicating that the vendor's system and procedures have been found to be in compliance with PCI-DSS by a firm that has been authorized by the Payment Card Industry to make such an assessment. A copy of this documentation should be submitted to the College IT Security Officer.

4. Each Person Who Has Access to Credit or Debit Card Information is Responsible for Protecting the Information

Individuals who have access to credit or debit card information are responsible for properly safeguarding the data and must comply with all requirements of the College's Information Security Policy to protect the integrity and privacy of such information. This policy can be found on the College's Website.
The following pieces of information are considered "confidential" within the meaning of the Information Security Policy and must be protected appropriately from initial capture through destruction regardless the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):

- Credit or debit card number

- Credit or debit card expiration date

- Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.

- Personal identification number (PIN)

- Cardholder's name, address and/or phone number when used in conjunction with the above fields

Neither the three- or four-digit credit or debit card validation codes (CVV2) nor Personal Identification Numbers (PIN) may ever be stored in conjunction with credit or debit card information in any form.

Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device.

Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days. While the documents are retained, they must be stored in locked cabinets in secured areas with access restricted to authorized individuals on a need-to-know basis. Keys that allow access to such containers must be immediately collected from any individual who leaves the College or whose responsibilities no longer require him or her to access such documents. When combination locks are used, the combination must be changed when an individual who knows the combination leaves the College or no longer requires access to perform assigned work. For any physical documents that contain credit or debit card information, it is strongly recommended that all but the last four digits of the credit or debit card number be physically cut out of the document. Overwriting the credit or debit card number with a marker is not acceptable since the number can still be viewed in certain circumstances.

No lists should be maintained that include entire credit or debit card numbers without the approval of the College IT Security Officer.

Credit or debit card information may be shared only with individuals who have been authorized to access such data by the appropriate Academic or Administrative Manager, Dean or Director.

5. Credit and Debit Card Information Must Be Destroyed as Soon as It is No Longer Necessary

All credit and debit card information must be destroyed as soon as it is no longer necessary, and may not be retained for more than 90 days after the transaction is processed.

All physical documents that are no longer necessary must be cross-cut shredded using a commercially available shredding device approved by the College IT Security Officer.

6. Departments Must Maintain Appropriate Checks and Balances in the Handling of Credit and Debit Card Information

Departments handling credit or debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit and/or debit card information. A system of checks and balances should be put in place in which tasks are performed by different individuals in order to assure adequate controls. For example, the same person should not process credit or debit card transactions/refunds and perform the monthly credit and debit card reconciliation. Where staffing permits, it is strongly recommended that the responsibility for processing transactions and refunds be segregated as well.

The Department Manager or his/her designee should not handle or have access to credit and debit card transactions. He or she will verify that the original supporting detail records agree with deposits on the General Ledger Journal. Terminal or web-based reports must not be the only supporting detail record.

The Department Manager or his/her designee is responsible for ensuring that Human Resources is aware of any job description changes that are made in support of maintaining the segregation of duties.

7. Each Department that Handles Credit and/or Debit Card Information Must Have Documented Procedures for Complying with this Policy and PCI-DSS.

Each department that handles credit and debit card information must have written procedures tailored to its specific organization that are consistent with this policy and PCI-DSS.

These departmental procedures will include, but are not limited to, the following:

□ Segregation of duties

□ Reconciliation procedures

□ Physical security

□ Disposal

□ Cash register procedures (if applicable)

8. Suspected Theft of Information Must Be Reported Immediately to the College IT Security, Business Office Manager and Campus Police Chief.

Any individual who suspects the loss or theft of any materials containing cardholder data, that person must immediately notify the College IT Security, Business Office Manager and Campus Police Chief.

Exceptions to Required Procedures

It is understood that a unique situation within an individual department may require a permanent or short-term exception to one or more of the above procedures. Such an exception must satisfy ALL of the following conditions:

□ It must comply with all applicable PCI-DSS requirements.

□ It must be approved by the College IT Security Officer and the Vice President of Administrative Financial Services and Business Manager.

□ In the case of a permanent exception, it must be included in a department's written procedures.

□ In the case of a short-term exception, it must be restricted to specific dates or events.