University of Virginia
Credit Card Requirements

The University of Virginia recognizes that e-commerce is critical for the efficient operation of the University, and in particular for collecting revenue. The University also recognizes that payment card information is highly sensitive data; failure to maintain strict controls over this information could result in unauthorized use of a credit card number and serious problems for the consumer, the merchant, and the University. We are committed to protecting this data, and these requirements assist the University in maintaining a secure environment and in complying with the required Payment Card Industry Data Security Standards (PCI-DSS).

Summary:

A University department or unit that is approved to host conferences or workshops, collect donations or gifts, and/or collect revenue from the sales of goods or services may choose to accept credit cards as a payment option. The requirements are also relevant to University revenues received from a third-party vendor that offers credit cards as a payment method. In this document, University departments and units that receive revenue from credit card processes are referred to as merchants.

The use of credit cards to collect University funds MUST be authorized by Payment Card Services (PCS) before contracts are signed, merchant accounts are obtained, or revenue resulting from payment card processing is received.

Cardholder data (CHD) is considered highly sensitive data and must be protected in accordance with University policy and industry requirements.

Merchants must comply with the PCI-DSS. These requirements are a contractual obligation to any entity involved in the processing, storage, or transmission of cardholder data or to those who receive revenue resulting from the processing of payment card transactions.

Payment cards include credit cards, debit cards, etc. that displays the logo of the major payment card brands: American Express, Discover, MasterCard, or Visa.

The ability to accept credit cards is a privilege. PCS reserves the right to suspend or terminate a merchant number and/or end credit card transaction acceptance to insure compliance with University requirements and the PCI-DSS, or if the merchant creates significant institutional risk that is not appropriately mitigated.

Contents:

- Section I - Guidance for University payment card processes.
  - General Information
  - Payment Card Methods
  - Payment Cards and Third-Party Vendors
  - Payment Card Processing
Section II – Overview of the Payment Card Industry Data Security Standards (PCI-DSS). The merchant is responsible for adhering to all of the standards in the PCI-DSS and for annually certifying their continued compliance by submitting the appropriate PCI-DSS Self-Assessment Questionnaire (SAQ) and supporting University-required documents.

Section III – List of the related University financial and electronic information policies and payment card resources.

Section I – University Card Requirements

General Information:

- All University departments and administrative units (merchants) are eligible to apply to process payment cards or accept revenue generated from payment card acceptance provided that they abide by University policies and procedures, and the PCI-DSS.

- University-related organizations (e.g.: University foundations) may apply for a University merchant accounts provided that they agree to abide by University policies, procedures, and the PCI-DSS.

- University merchants cannot negotiate their own contracts with credit card processing companies or third-party vendors accepting payment card payments on their behalf, including zero-dollar purchase orders and acceptance of on-line click-through agreements (EULAs).

- The University of Virginia has contracted with MasterCard, Visa, American Express and Discover Cards. Merchants normally accept all four cards.

- All costs for transaction fees, website development, equipment, or operations associated with conducting these transactions will be borne by the merchant along with any fees and penalties associated with failures to comply with University requirements or PCI Standards. The merchant must determine if sales tax must be charged for goods or services sold (Policy FIN-032).
Payment Card Methods:

There are two commonly accepted methods for processing transactions; web-based payments made by customers through University-approved gateways, and point-of-sale transactions via approved payment card ‘swipe terminals’.

• Web-based Payments: These are payments made by a customer through a secure and University approved payment gateway website (EPay@UVA, QuikPay, Apply Yourself, etc.).
  o In designing online payment processes, a client’s payment cardholder data must NEVER be entered into web forms or stored in any non-approved systems or electronic documents prior to passing the customer on to a University authorized payment gateway (third-party hosted, PCI compliant website).
  o Merchant personnel should NEVER enter a client’s payment card data into a website on behalf of the client. This is in compliance with PCI-DSS and helps to protect the University and our clients from the possibility of data loss due to spyware and keyboard “sniffers”.
  o A merchant planning to process credit cards through a link on their website will be responsible for designing (or contracting with a web developer to design) a PCI compliant departmental webpage to hand-off to a PCS approved gateway.
  o A merchant webpage must contain the merchant’s refund policy and the University’s privacy policy as well as department/unit contact information (for payer questions) prior to the gateway.
  o The website and server on which it resides must comply with PCI-DSS.

• Point-of-Sale (PoS) Terminal Payments:
  o Merchants must obtain PoS terminals from PCS, not from outside vendors.
  o Merchants using card swipe terminals must follow the transaction processing guidelines as outlined in the merchant operating guide and comply with PCI-DSS requirements.
  o Merchants using card swipe terminals must follow the transaction processing guidelines as outlined in the merchant operating guide and comply with PCI-DSS requirements.
  o Only PCS approved cellular-based wireless swipe terminals are options for mobile processing (not smart phones, tablets, Wi-Fi enabled devices, etc.).
  o Swipe-terminals must be tamper-proof, and inspected before daily use.
  o Equipment that does not meet the above criteria must be kept in a locked safe/cabinet or covered with a lockable shroud when not in use or if left unattended.
  o Swipe-terminals must
  o Be EMV Chip and PIN enabled by October, 2015.

• Mobile payment processes through Class III personal devices (such as smart phones, tablets, etc.) coupled with payment applications (apps) or attached hardware (i.e.: Square, GoPayment, etc.) are not authorized for use at this time.
• Other methods such as stand-alone computer systems, software applications, integrated payment register systems, and use of third-party payment card processors are not permitted unless authorized by PCS.

• Software applications including all purchased, custom applications, and self-developed software, including internal and external (web) applications, and computer-based applications must be PA-DSS compliant (the PCI Council’s Payment Application Data Security Standards).

Payment Cards and Third-Party Vendors:

The University is obligated to understand cardholder data flow and verify the PCI compliance of any third-party who processes or collects payment card revenue on its behalf. The scope of PCI spans from the workstation, through to the network to payment web pages and systems.

• PCI-DSS requires us to insure that any software providers or third-party payment card partners (those associated with the University that are handling credit cards on our behalf or that we are recommending to our customers) are also PCI compliant in order for us to continue to utilize their services.

• When business requirements recommend the use of a third-party payment card processor (e.g. CyberSource), PCS in conjunction with Procurement & Supplier Diversity Services may authorize alternate methods.

Payment Card Processing:

• Merchants must NEVER request or process payment card payments by email. Cardholder data in emails must be securely deleted and the payer should be provided with an approved alternate payment method.

• Credit card transactions should be processed as soon as possible. Once processed, the cardholder data must be securely destroyed by cross-cut shredder, pulping, or hole-punching. Marking through the account number with pens or permanent markers is not sufficient.

• Credit card information that is not processed immediately must be stored in locked cabinets or non-portable safes. Do NOT leave completed forms unmonitored in open areas, mail boxes, envelopes, folders, or on desks. This information is highly sensitive data and must be protected according to the University Physical Records Storage Standards http://www.virginia.edu/recordsmanagement/standards/storagestandards.html. For example, “Two levels of protection – ex. locked file cabinet plus locked door or person sitting in the same room controlling access. File cabinets need to be locked at all times (not left open during work day). If person leaves location, locking of all access doors to rooms required.”
• Under **NO** circumstances should a merchant enter another person’s cardholder data electronically. This includes temporary (not saved) data entry into Excel files, databases, websites, Word documents, etc. without written approval from PCS.

• Merchants must develop payment card processing “desk-top” procedures that comply with University and PCI Standards. Procedures need to be step-by-step procedures, not broad policy statements. Completed procedures must include:
  - handling of email delivery;
  - inspecting equipment for tampering, if applicable;
  - approved methods for destroying CHD documents, forms, or related payment card information;
  - reporting violations of procedure and data breaches and network drawings, if applicable.

• When a refund is necessary for an item or service paid by payment card, the refund must be credited to the same credit card account from which the purchase was made.

• Payment card activities should be documented in the merchant’s UVA I.T. Security Risk Management (ITS-RM) plan.

**Payment Cards & Students-related Processes:**

• Credit cards payments for degree course registration, or most other student-related charges included on the student bill, are processed in the Student Information System (SIS) through the University’s online QuikPay@UVA system.
  - New student fees may require Board of Visitor or Dean’s approval, and they must be approved by Student Financial Services to be included on the student bill through SIS.

• Student Contracted Independent Organizations (CIOs) are excluded from use of University merchant accounts.

**Payment Cards and Personnel:**

• University merchants must appoint or work with an existing University-trained PCI Coordinator to help assure compliance with University requirements and PCI-DSS requirements.
  - The PCI Coordinator serves as a single point of contact and is responsible for training, compliance, desktop procedures, and submission of the SAQ.
  - Each merchant’s PCI Coordinator must complete the U.Va. PCI Coordinator Training. Contact PCS to register for a session.

• Personnel involved in the processing, storage, or transmission of payment card data must complete PCI frontline training annually and review their department’s payment card desktop procedures.
Completion is indicated by signing a [UVA Payment Card Confidentiality Agreement](mailto:U.Va._payment_card_svcs@virginia.edu). Completed agreements must be maintained by the merchant for audit purposes.

- All personnel who have direct access to payment card information (online or paper copies) are required to complete the Responsible Computing Tutorial for UVa Faculty & Staff at [https://whois.virginia.edu/security](https://whois.virginia.edu/security).
- All changes in processing methods or key personnel (PCI Coordinator, signatory authority, etc.) must be communicated to PCS timely.
- Volunteers, students, and part-time/temporary employees should be supervised by permanent staff when CHD must be handled.
- PCI requires that any personnel who have access to multiple card data at a single time or have the ability to issue credits must have completed a background check.

**Payment Card Storage:**

- Prior to storing payment card data for required business practices, it must be limited to the payer’s name and the last 4 digits of the Primary Account Number (PAN).
- A merchant should never store sensitive authentication service/security code data (sometimes known as the CVV2 code) electronically or in hard copy.
- If cardholder data (i.e.: the full credit card number) must be retained for unavoidable business requirements, it must be approved by PCS and the University’s Information Security, Policy, and Records Office (ISPRO). The University’s Electronic Storage of Highly Sensitive Data policy [https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-015](https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-015) also states that storage of such highly sensitive data on an individual-use device requires a Vice President’s or Dean’s written permission as well as heightened security requirements, including encryption. Storage of such data on a server requires compliance with the data protection standards for highly sensitive data [http://www.virginia.edu/informationsecurity/dataprotection](http://www.virginia.edu/informationsecurity/dataprotection).
- Track data (data from the card’s magnetic stripe) captured through card terminals or other processes must never be retained after card authorization, even if encrypted.
- Use appropriate facility entry controls to limit and monitor physical access to records and/or systems that store, process, or transmit cardholder data. Access should be limited to only those employees who need this information to accomplish their work. Make sure all visitors are authorized before entering areas where cardholder data is processed or maintained.
  - In areas where CHD is present, arrange for cleaning services when authorized personnel can provide oversight (not after hours).
• Logs are required for the movement of stored records containing cardholder data.

**Payment Cards - Computers and Related Equipment:**

• Departments must assure that all computers that handle credit card data possess the most recent updated versions of University recommended anti-virus and spyware detection software.

• Departments must also run University recommended sensitive data detection software at least once a month to insure that payment card data is not resident on the computer.

• FAX machines are an acceptable way to receive payment card information, provided that they are in a secure location and MUST be programmed not to print during outside business hours when authorized personnel are present.

• Computers made available to students and/or general public must have a visible UVA ‘Indemnity’ Statement relating that the machines are not secure for payment card processes, particularly in an area where credit card processing over the web is accepted.

• Customers should not be directed to use a specific computer to conduct a payment card payment.

• The PCI requirements apply to all “system components” involved in payment card activities, which is defined as any network component, server, or application included in, or connected to, the cardholder data environment.
  o Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, NS, mail, proxy, and NTP.

**Payment Card Accounting and Reconciliations:**

• The merchant must have a PTAO where fees will be charged.

• All revenue generated through the sale of goods or services must be deposited into the University’s bank account unless authorized by PCS.

• All transactions involving University funds must be settled and recorded in the Integrated System in a timely manner and reconciled in accordance with University policies and procedures.

• Duties must be properly segregated to comply with University Internal Controls, i.e.: reconcilers should not be able to initiate refunds.

**Reporting Suspected Data Breaches or Failed PCI Compliance:**

It is essential to report suspected breaches of payment card data or violations of PCI and University requirements as soon as possible. Most employees should
contact their PCI Coordinator, who will initiate the report to Information Security Policy & Records Office (ISPRO).

- Departments must report any actual or suspected security incident in which cardholder information may have been compromised.

- The incident should be reported to the ISPRO as required by University Policy IRM-012, Information Incident Security Reporting.

- **TO REPORT INFORMATION SECURITY INCIDENTS:**
  - Complete the online form at: http://www.virginia.edu/informationsecurity/reporting.html
  - Notify the University police department http://www.virginia.edu/uvapolice/contact.html as quickly as possible.
  - This MUST be done within 24 hours of detection.

**Section II- Payment Card Industry Data Security Standards (PCI-DSS)**

The Payment Card Industry data security standards are technical and operational requirements set by the PCI Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data; there are additional requirements for software developers and manufacturers of applications and devices used in those processes. Compliance with the PCI set of standards is mandatory for their respective stakeholders.

The PCI Security Standards Council is an independent body created by the major payment brands (American Express, Discover, MasterCard and Visa) to be the governing organization and open forum responsible for the development, management, education, and awareness of PCI Security Standards, including the Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS). The Council also develops and manages a number of programs to train, test, and qualify organizations and individuals to assess and validate adherence to PCI Security Standards. The payment brands and the acquirers are responsible for enforcing compliance, not the PCI Council.

The University and its merchants have a contractual obligation to adhere to the PCI Data Security Standard (PCI-DSS), non-compliance is not an option. The card brands and credit card processors can assess significant fines for failure to comply with the PCI-DSS and can revoke the University’s ability to accept payment cards.

Each University merchant is responsible for:
- Adhering to all of the PCI-DSS standards
- Any associated costs with non-compliance or if a breach occurs, i.e.: forensics, fraud, replacement cards, credit monitoring, etc.
• Annually certifying their continued compliance by completing the PCI-DSS Self-Assessment Questionnaire (SAQ) appropriate to their credit card activities and signed by the head of the college, business unit or department.

• Passing quarterly vulnerability scan” and an annual penetration test for all web sites in the merchant credit card environment.
  o The testing is arranged by PCS and conducted by an Authorized Scanning vendor.

The PCI Standards and annual SAQ questions span the following six goals, which are then sub-divided into 12 Requirements. Each requirement has several very detailed sub-requirements which also must be followed.

**PCI-DSS Goals and Requirements:**

**BUILD AND MAINTAIN A SECURE NETWORK**
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

**PROTECT CARDHOLDER DATA**
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

**MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM**
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

**IMPLEMENT STRONG ACCESS CONTROL MEASURES**
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

**REGULARLY MONITOR AND TEST NETWORKS**
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

**MAINTAIN AN INFORMATION SECURITY POLICY**
- Requirement 12: Maintain a policy that addresses information security

In-depth information on the PSI-DSS can be found on the PCI Council’s website: [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org).

**Section III – Contacts & Policy References**

**Contact Offices:**

Payment Card Services - [http://www.virginia.edu/finance/ecommerce](http://www.virginia.edu/finance/ecommerce)
Email: uva_payment_card_svcs@virginia.edu
Email: it-security@virginia.edu

Related University Policies:

V.A.1 - Revenue Generating Activities
  • http://www.virginia.edu/finance/polproc/pol/va1.html
FIN-021 - Internal Control
  • https://policy.itc.virginia.edu/policy/policydisplay?id=FIN-021
FIN-032 - Collecting, Reporting and Remitting Virginia Sales Tax
  • https://policy.itc.virginia.edu/policy/policydisplay?id=FIN-032
GOV-002 – Reporting Fraudulent Transactions
  • https://policy.itc.virginia.edu/policy/policydisplay?id=GOV-002
IRM-003 – Information Technology Security Risk Management Program
  • https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-003
IRM-012 – Information Technology Security Incident Reporting
  • https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-012
IRM-015 - Electronic Storage of Highly Sensitive Data
  • https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-015

Electronic Information Resources:

Responsible Computing Handbook for Faculty and Staff

Responsibilities for Computing Devices Connected to the University Of Virginia Network
http://www.itc.virginia.edu/policy/netdevices

Ethics in Computer Usage
http://wwwtest.itc.virginia.edu/policy/ethics.html

Information Policy at UVa
http://www.virginia.edu/informationpolicy

University Of Virginia Administrative Data Access Policy
http://www.virginia.edu/informationpolicy/admindataaccess.html

Information Technology Security Risk Management (ITS-RM) Program
http://www.virginia.edu/informationsecurity/riskmanagement

Electronic Storage of Highly Sensitive Data Policy
https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-015

University Data Protection Standards
http://www.virginia.edu/informationsecurity/dataprotection/

University Physical Storage Standards
http://www.virginia.edu/recordsmanagement/standards/storagestandards.html