

University of Virginia Credit Card Guidelines

A University department that is approved to sell goods or services may choose to accept credit cards from its customers as a payment option (see related policies in Section Three). This document provides operating guidance to units, which are defined as departments, offices, and all other entities that accept or want to accept payments by credit cards. These guidelines also apply to departments that accept credit card information for activities such as fund raising to be passed on to another department for processing. This should be considered University operating policy until such time as it is replaced by a credit card policy.

The document consists of three sections. The first section provides general guidance for University credit card operating policies. The second section describes the Payment Card Industry Data Security Standards (PCI-DSS). These are national standards from the Card Association and apply to all organizations anywhere in the country that process, transmit or store credit cardholder data. The University and all departments that process payment card data have a contractual obligation to adhere to the PCI Data Security Standard (PCI-DSS). We must adhere to these standards to limit our liability (and continue to process payments using payment cards). The standards listed in Section two are not a complete list, but only those most likely to occur in a University environment. The department is responsible for adhering to all the standards in the PCI-DSS. Section three is the list of the related University financial and electronic information policies.

Also for the purpose of this document as it applies to the University, the term “merchant” will refer to any University department that has contracted to accept payment for goods and services in the form of a credit card.

Section I

Credit cards may only be accepted for goods, services, non-degree course registration, fees, and gifts to the university.

Departments cannot negotiate their own contracts with credit card processing companies. All merchant accounts for accepting credit cards must be approved by the Comptroller’s Office.

A University department (unit) that is approved to sell goods or services (see other policies for further detail) may choose to accept credit cards from its customers as a payment option. Credit cards may only be accepted for goods, services, non-degree course registration, fees, and gifts to the University.

The department is responsible for all expenses associated with credit card merchant accounts and it can not adjust the price of goods or services based upon the method of payment.

All revenue generated through the sale of goods or services must be deposited in the University's bank account unless authorized in writing by the Comptroller's Office

There are two accepted methods for processing transactions: (1) secure website through the University gateway and (2) card swipe terminal. Other methods such as stand-alone systems are not permitted unless authorized in writing by the Comptroller's Office.

A department wishing to allow its customers to use credit cards over the web will be responsible for designing (or contracting to design) a departmental website. The website will be used to collect all essential data required to process a customer request. The credit card information must not be stored or entered in the unit's website. The website and credit card processing must be designed in accordance with the Payment Card Industry Data Security Standards (see below) and the University Web Site Policy (<http://www.virginia.edu/copyright.html>).

Individual credit card information is confidential; 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 unit and the University. Credit card information, therefore, should be treated as carefully as any other confidential information (see Payment Card Industry Data Security Standards below).

- **Under no circumstances should a department retain electronically (including excel files) the credit card numbers and expiration dates of customer credit cards.**
- **Never send or request cardholder information to be sent via unencrypted e-mail**
- **Customer records located within units should be stored in locked cabinets.**
- **Access should be limited to only those employees who need this information to accomplish their work.**
- Do not store sensitive authentication data (track from the Magnetic stripe, card-validation code CVV2 data or PIN numbers) subsequent to authorization (not even if encrypted).
- If sensitive cardholder data (i.e. the credit card number) must be retained for operating purposes, it must be rendered unreadable by encryption anywhere it is stored.
- Make sure all visitors are authorized before entering areas where cardholder data is processed or maintained.
- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
- Do not use wireless PC's for processing credit card data unless approved in writing by the director of communications and systems.

Departments using the card swipe terminals must follow the transaction processing guidelines as outlined in the NOVA Merchant Operating Guide

The department must determine if sales tax must be charged for goods or services sold.

When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the same credit card account from which the purchase was made.

All transactions must be settled and recorded daily in the university financial records. Departments also must reconcile their clearing activity at least monthly.

Departmental personnel must reconcile transactions captured/processed through the terminal/web processor with the sales transactions posted to the unit/University records.

All personnel who have direct access to on-line credit card information are required to take the Security Awareness at UVa. test at <https://whois.virginia.edu/security>.

Departments must report any actual or suspected security incident in which cardholder information may have been compromised. The incident should be reported to Internal Audit, and the Comptroller's office. If the security incident involved electronic stored or processed data, it must also be reported to the Director of Security Coordination and Policy in the Office of Information Technology and Communication.

TO REPORT ELECTRONIC SECURITY INCIDENTS EMAIL: abuse@virginia.edu

Section II

Payment Card Industry Data Security Standard

Note that these Payment Card Industry (PCI) Data Security Requirements apply to all departments/merchants that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. 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. Applications include all purchased and custom applications, including internal and external (web) applications and PC applications.

In depth information on the PSI-DSS can be found on the following website:
www.visa.com/cisp

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data.

All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access.

- Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- Always change the vendor-supplied defaults **before** you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts).
- Configure system security parameters to prevent misuse

Protect Cardholder Data

Requirement 3: Protect Stored Data

- Do not store sensitive authentication data subsequent to authorization (not even if encrypted):
- Keep cardholder information storage to a minimum.
- Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
- Do not store the full contents of any track from the magnetic stripe (on the back of a card,

- in a chip, etc.)
- Do not store the card-validation code (Three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data) or the PIN Verification Value (PVV)
- Mask account numbers when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks.

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit.

- **Never send cardholder information via unencrypted e-mail**
- Use strong cryptography and encryption to safeguard sensitive cardholder data during transmission over public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs.

Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.

- Deploy anti-virus mechanisms on all systems commonly affected by viruses (e.g. PC's and servers).
- Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

- Ensure that all system components and software have the latest vendor-supplied security patches.
- Install relevant security patches within one month of release.
- Establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.
- Develop software applications based on industry best practices and include information security throughout the software development life cycle.
- Follow change control procedures for all system and software configuration changes.
- Develop web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines.

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know.

Ensure critical data can only be accessed in an authorized manner.

- Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

- Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Requirement 8: Assign a unique ID to each person with computer access.

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

- Identify all users with a unique username before allowing them to access system components or cardholder data.
- Encrypt all passwords during transmission and storage, on all system components.
- Remove inactive user accounts at least every 90 days
- Distribute password procedures and policies to all users who have access to cardholder information
- Do not use group, shared, or generic accounts/passwords
- Change user passwords at least every 90 days
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted.

- **Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.**
- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
- Restrict physical access to wireless access points, gateways, and handheld devices.
- Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.
"Employee" refers to full-time and part-time employees, temporary employees/personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- Make sure all visitors are authorized before entering areas where cardholder data is processed or maintained
- Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information
- Maintain strict control over the storage and accessibility of media that contains cardholder information:
 - Properly inventory all media and make sure it is securely stored.
 - Destroy media containing cardholder information when it is no longer needed for business or legal reasons:
 - Cross-cut shred, incinerate, or pulp hardcopy materials
 - Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong.

Requirement 11: Regularly test security systems and processes

Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and through changes.

- Test security controls, limitations, network connections, and restrictions routinely to make sure they can adequately identify or stop any unauthorized access attempts. Where wireless technology is deployed, use a wireless analyzer periodically to identify all wireless devices in use.
- Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Perform penetration testing on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to environment, web server added to environment).
- Use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

- Ensure the security policy and procedures clearly define information security responsibilities for all employees and contractors.
- Make all employees aware of the importance of cardholder information security.
- Require employees to acknowledge in writing they have read and understood the company's security policy and procedures.
- Implement an incident response plan. Be prepared to respond immediately to a system breach.
- Provide appropriate training to staff with security breach response responsibilities.

Section III

POLICY REFERENCES

University Policies:

- I.A.1-Internal Controls
- V.A.1-Revenue Generating Activities
- GOV-002 – Reporting Fraudulent Transactions
- IRM-003 – Information Technology Security Risk Management Program

Electronic Information Policies:

RESPONSIBLE COMPUTING HANDBOOK FOR FACULTY AND STAFF
<http://www.itc.virginia.edu/pubs/docs/RespComp/resp-comp-facstf.html>

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>

UNIVERSITY COMPUTING POLICY DIGEST AND RELATED INFORMATION
<http://www.itc.virginia.edu/policy/>

ELECTRONIC DATA REMOVAL FROM UNIVERSITY-OWNED AND
CONTROLLED COMPUTERS
<https://etg07.itc.virginia.edu/policy/policydisplay?id=%27IRM-004%27>

UNIVERSITY OF VIRGINIA ADMINISTRATIVE DATA ACCESS POLICY
<http://www.itc.virginia.edu/policy/itcadminnew.htm>

INFORMATION TECHNOLOGY SECURITY RISK MANAGEMENT (ITS-RM)
PROGRAM
<http://www.itc.virginia.edu/security/riskmanagement/>

Please contact Ken Sinarski (kens@virginia.edu) at 924-4877 or B.C. Worsley (bsw5w@virginia.edu) at 924-4362 if you need additional information.