The University of Vermont

OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

Title: Accepting Payment Cards and eCommerce Payments

Policy Statement

The University of Vermont limits the acceptance of credit and debit cards, referred to collectively as payment cards, to those departments who are given authority by the Controller's Office. Permission to accept payment cards is based upon volume of payments and existing internal controls. In order for a department to accept payment cards, it must become a UVM-authorized Merchant, as defined below. In doing so, the department must commit to adhere to the Payment Card Industry Data Security Standards (PCI DSS).

Reason for the Policy

The University of Vermont's acceptance of payment cards for gifts, goods, and services has been growing over the past several years. Increased interest in accepting payments over the internet (e-commerce) has also grown, spurring the need to establish business processes and policies that protect the interests of the University and its customers.

While the costs for accepting payment cards can be significant (approximately 1.5%–3.0% of every transaction, depending on the card type), it often makes sense to accept this type of payment for business reasons, which include control of receivables, competitive position, and efficient processing. To the extent that it makes economic sense, the University wishes to support this activity. In order to ensure that payment card activities are consistent, efficient, auditable, and secure, the University has adopted the following policy and supporting procedures for all types of payment card activity transacted in-person, over the phone, and via fax, mail, or the internet.

This policy provides guidance so that credit card acceptance and e-commerce processes can comply with PCI DSS and are appropriately integrated with the University's financial and other systems.

Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines, possible legal liability, and the potential loss of the ability to accept credit card payments.

The University of Vermont has contracted with a third-party vendor ("Authorized Vendor"), as designated by the Vice President for Finance and Administration, whose core business includes the support and processing of e-commerce transactions. The Authorized Vendor will provide the University with a secure gateway and hosted solution in which all payment card and personal payment information is transmitted to and stored on off-site computers that the Authorized Vendor owns and maintains. The Authorized Vendor must maintain PCI DSS compliance certification. This relationship will enable the University to leverage the volume of e-commerce transactions and reduce processing costs.

Applicability of the Policy

Any University of Vermont employee, contractor, or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of payment card and/or e-commerce payments for the University is subject to this policy.

Definitions

Authorized Vendor: A third-party vendor with PCI Compliance Certification as selected by the Controller's Office to provide the University with a secure gateway and hosted solution in which all payment card and personal payment information is transmitted to and stored on off-site computers owned and maintained by the Authorized Vendor.

Merchant: A University department or unit that has been approved by the Controller's Office to accept payment cards and electronic payments for gifts, goods, and/or services.

Merchant Department Responsible Person (MDRP): The person within each Merchant department who is responsible for managing credit card and/or e-commerce transaction processing, as well as ensuring that the Merchant department stays in compliance with PCI DSS by completing, or delegating, the yearly Self-Assessment Questionnaire (SAQ).

Payment Card Industry Data Security Standards (PCI DSS): A uniform set of data security standards developed by the major credit card companies (VISA, MasterCard, Discover, and American Express) with which everyone that stores, processes, or transmits cardholder data must comply (https://www.pcisecuritystandards.org/). Non-compliance with PCI DSS standards puts the University at risk for:

- Large monetary fines assessed to the Merchant and/or the University
- Loss of merchant status for department
- Loss of merchant status for the University
- Harm to the University of Vermont's reputation

Self-Assessment Questionnaire (SAQ): A Questionnaire that is designed as a self-validation tool to assess security for cardholder data. It consists of a set of questions corresponding to the PCI Data Security Standard requirements, as well as an Attestation of Compliance or certification that you have performed the appropriate Self-Assessment.

Procedures

Any department accepting payment card and/or electronic payments on behalf of University of Vermont for gifts, goods, or services ("Merchant") must designate an individual within that department who will have primary authority and responsibility for e-commerce and credit card transaction processing within that department. This individual will be referred to in the remainder of this policy statement as the Merchant Department Responsible Person or "MDRP."

Failure to comply with the terms of this policy may result in disciplinary actions, including possible termination of employment, and could also limit a department's payment card acceptance privileges. Disciplinary provisions for represented employees shall follow those policies contained in existing collective bargaining agreements. Noncompliance by a contractor or agent may result in a breach of contract and/or termination of a contract or agency agreement.

All MDRPs must:

1. Execute on behalf of the relevant Merchant the "Procedures to Initiate Acceptance of Payment Cards and e-Commerce Payments" detailed below.

2. Inform, in writing, all employees (including the MDRP), contractors, and agents with access to payment card data within the relevant Merchant Department that they must read, understand, and comply with this Policy for Accepting Payment Cards and e-Commerce Payments.

3. Complete the appropriate PCI DSS Self- Assessment Questionnaire (SAQ) for the Merchant on an annual basis, register IP address(es), and conduct required quarterly vulnerability scans, as applicable. A current SAQ must be certified by a Dean, Director, Chair or designee, completed within the past twelve months, and kept available for inspection.

4. Ensure that all payment card data (including, but not limited to, account numbers, card imprints, and Terminal Identification Numbers [TIDs]) collected by the relevant Merchant in the course of performing University of Vermont business, regardless of how the payment card data is stored (physically or electronically), is secured at all times. Data is considered to be secured only if the provisions of the University's Information Security and Privacy Policy, and PCI Data Security Standards are followed. Some of the criteria include:

    - Only those with a need-to-know are granted access to payment card and electronic payment data.

    - Email should not be used to transmit payment card or personal payment information. If it should be necessary to transmit payment card information via email, only the last four digits of the payment card number can be displayed.

    - Payment card or personal payment information is never downloaded onto any personal portable electronic devices such as smart phones, USB flash drives, laptop computers or other digital media.

    - Fax transmissions (both sending and receiving) of payment card and electronic payment information occurs only on those fax machines to which access is restricted to just those individuals who must have contact with payment card information in order to do their jobs.

    - The processing and storage of personally identifiable payment card or payment information on University computers and servers is prohibited, except as provided in this policy. Exceptions can only be made if the processing and storage methods are compliant with this policy and the aforementioned policies and standards. These standards detail strict encryption protocols. (NOTE: University of Vermont's Information Security Office maintains a staff of security professionals who are available, as required, to provide consultative services on appropriate security practices. The Information Security Office can be contacted at ISO@list.uvm.edu, or 656-2123 or (866) 236-5752.

    - Only secure communication protocols and/or encrypted connections to the Authorized Vendor are used during the processing of e-commerce transactions.

    - Only encrypted connections are used for the internal transmission of data.

    - The three-digit card-validation code printed on the signature panel of a credit card is never stored in any form.

    - The full contents of any track from the magnetic stripe (on the back of a credit card, in a chip, etc.) are never stored in any form.

- All but the last four digits of any payment card account number are always masked, should it be necessary to display payment card data.

- All media containing payment card and personal payment data that are no longer deemed necessary or appropriate to store are destroyed or rendered unreadable, in accordance with other University policies concerning retention of records.

Merchants must use the services of the Authorized Vendor to process all e-commerce transactions. If a Merchant believes that it has a significant business case or processing requirement that cannot be achieved using the services of the Authorized Vendor and wishes to utilize an alternative, it must initiate its request in writing to the Director of Treasury Services for a release from the Authorized Vendor requirements specified by this policy. The Director of Treasury Services will forward the request to the Controller and Chief Information Officer (CIO) with a recommendation. Only the Controller and CIO may jointly authorize, in writing, the adoption of alternative e-commerce vendors and products.

In the event that the Controller and CIO authorize the use of an alternative e-commerce vendor, then the following must occur:

- The MDRP must provide proof initially, and annually thereafter, that the alternate e-commerce vendor is certified as PCI compliant; and

- The MDRP must ensure that the department and its vendor comply with all relevant provisions of the University's Information Security and Privacy Policy, PCI DSS, and this Policy for Accepting Payment Cards and e-Commerce Payments.

In accordance with merchant agreements with card companies, the following requirements apply to all University Merchants:

- All Merchants accepting Visa, MasterCard, American Express, and/or Discover Card shall promptly honor all such valid transactions and will not establish minimum amounts (except as permitted by law) or maximum transaction amounts.

- All Merchants shall not select what sales or services may be charged by a cardholder. All sales or services provided at that location can be charged at the option of the cardholder.

- All transactions must be pre-authorized and when a cardholder is present a sales draft must be signed by the cardholder.

- All Merchants must exercise reasonable diligence to the best of their ability in determining that the signature on the sales draft is the same as the authorized signature on the card.

- All Merchants will establish a reasonable and fair policy for exchange and returns and give proper credit or issue credit vouchers.

- All Merchants must exercise reasonable diligence to the best of their ability in determining whether fraudulent or unauthorized use of a credit card has occurred.

By becoming a Merchant, the unit agrees to:

- Be charged a merchant fee for all credit card transactions calculated at a predetermined rate. A lower rate is charged for cards that are physically present and swiped through the terminal.

- Be charged a per-transaction fee for all transactions processed through the Authorized Vendor for e-commerce transactions, and a fixed monthly amount for hosting/maintenance.

- Be charged an annual fee through the merchant bank processor with which the University of Vermont has a banking relationship.
- Balance, settle, and close their credit card terminal daily, including weekends.
- Maintain the original sales draft for at least 30 days. Maintain a copy of the sales draft for a minimum of two years, acknowledging a chargeback may occur for up to seven years.
- Process payment credit card transactions through the merchant bank processor with which the University of Vermont has a merchant banking relationship.

By becoming a Merchant, the unit agrees to follow security best practices as prescribed by PCI Data Security Standards, such as:

- Mask all but the last four digits of any payment card account on the sales draft in order to protect such cardholder data.
- Use anti-virus software that is kept updated automatically.
- Not use vendor-supplied defaults for systems passwords and other security parameters; change systems passwords when key personnel associated with credit-card processing leave positions with Merchant.
- Assign a unique ID to each person with computer access, including student employees.
- House computer systems that process payment cards behind a firewall with the highest level of protection consistent with the system's access requirements.
- Use computer systems that process payment cards with the ability to monitor and track access to network resources, the computer itself, and cardholder data.
- Report all suspected or known security breaches in accordance with "Procedures for Responding to a Security Breach," below.
- Develop practices and procedures consistent with any applicable existing policy of the University related to information security and privacy, and the retention or destruction of records.

Procedures to Initiate Acceptance of Payment Card and eCommerce Payments

The MDRP or their designee must follow the steps below in order to initiate payment card processing and e-commerce at the University of Vermont.

1. Complete an Application to Become a Merchant. Applications must be signed by the MDRP as well as the college/school/division Budget Manager. It is the responsibility of the Budget Manager to approve the business case for the department to become a merchant department, the PeopleSoft information provided, and the designated Merchant Department Responsible Person.
2. Submit the application for review and approval to Treasury.Management@uvm.edu. Allow two to four weeks for processing of the request. All applications require the approval of the Director of Treasury Services.

If the application is approved, any necessary equipment will be obtained from the merchant acquiring bank at the expense of the Merchant Department. Training on accessing the daily settlement for depositing purposes will be provided upon request by Treasury Services.

Procedures for Responding to a Security Breach

The MDRP or individual suspecting a security breach must follow the University's Breach Notification Procedures developed to comply with An Act Relating to the Protection of Personal Information (9 V.S.A. chapter 62). Report a data breach to the UVM Information Security Office by calling the toll-free number (866) 236-5752 or the internal UVM number 656-2123.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Treasury Services Office	Treasury.Management@uvm.edu
Director of Treasury Services	(802) 656-2236
Senior Treasury Professional	(802) 656-3223
Treasury Professional	(802) 656-5850

Forms/Flowcharts/Diagrams

- Application to Become a Merchant

Related Documents/Policies

- Computer, Communication, and Network Technology Acceptable Use Policy
- Information Security Policy
- Privacy Policy

Regulatory References/Citations

- American Express Merchant Reference Guide
- Card Acceptance Guidelines for Visa Merchants
- Discover Network for Merchants
- MasterCard Rules Manual

Training/Education

Training will be provided on an as-needed basis as determined by the Approval Authority or the Responsible Official.

About this Policy

Responsible Official:	Vice President for Finance and Administration	**Approval Authority:**	President
Policy Number:	V. 4.1.3	**Effective Date:**	March 16, 2018
Revision History:	• V. 4.3.9.1/V. 4.1.1 effective September 29, 2010 • V. 4.1.3 approved June 22, 2022		