O

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 (eCommerce) 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%-3.5% of every transaction, depending on41 (sn)-1 ( )]T4 1 (ns)2.ty agde.

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 e-commerce payments for the University

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 previous 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 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 only 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) 236-6752.

    -

- 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 a 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 alternative 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 xercdh(ascredit vouchers.

- 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 [illegible]