University of Massachusetts
Amherst
Controller's Office
405 Goodell Building
140 Hicks Way
Amherst, MA 01003-9334

phone: 413.545.1675
fax: 413.545.6088

Amherst Campus Credit Card Information Policy

1. Accepting Credit Card Payments

    a. Schools and departments planning to accept debit and credit cards must first contact the Amherst campus e-Commerce representative. The campus E-Commerce representative must approve any decisions to accept debit and credit cards or other electronic forms of cash receipts.

    b. The Amherst campus e-Commerce representative, Amherst campus bursar, and Amherst campus Information Security Officer will work with departments to provide the necessary guidance in the areas of PCI DSS (Payment Card Industry Data Security Standard) Compliance, internal controls, deposit techniques and reconciliation procedures.

    c. Bank accounts, debit and credit card accounts may only be opened by the University Treasurer's Office. "PayPal" accounts and other web-based payment mechanisms are not permitted for conducting university business unless approved by the Amherst E-commerce representative and Treasurer's Office.

    d. CyberSource has been identified as the third party processing vendor of choice for web-based e-commerce activity. See below for use of alternative third-party systems.

    e. All broken and discontinued POS terminals must be returned to the University Treasurer's office in a secure manner.

    f. All new credit card processing is potentially subject to a Qualified Security Assessor review at the expense of the department.

    g. Anyone in the department with access to credit card data, including any locked storage for physical records, must undergo annual ecommerce training.

    h. If you suspect that card data, whether paper or electronic, or systems processing data have been compromised, contact your campus e-Commerce representative immediately. Notify them of the suspect activity and await further instructions.

2. Storing Credit Card Data Electronically

    a. Departments are prohibited from storing sensitive cardholder data including the 16 digit credit card number, the CVV2 number (3 digit value printed on the signature panel of payment card) or PIN data on any computer, database, network,or file

without prior approval from the University's Treasurer's Office, and Amherst Campus Controller. Electronically storing sensitive cardholder data exposes the campus to potential identity theft as well as substantial penalties for lost or stolen data.

1. This includes the copying, moving and storage of cardholder data onto local hard drives and removable electronic media, regardless of how the data are accessed.

b. Requests to electronically store sensitive cardholder data must be signed by the Dean and Department Head and submitted to Campus eCommerce Manager. Schools and departments will be responsible for all fines and penalties relating to loss or theft of credit card data.

c. Departments storing credit card data electronically must submit to and comply with PCI compliance standards.

3. Storing Credit Card Data on Paper Forms or Reports

a. At times, departments receive credit card information filled out on order forms, faxes, etc. as part of conducting university business. In addition, sensitive credit card data may be printed on daily logs, reports and receipts. Departments should redact any sensitive cardholder data printed on paper by blacking out, photocopying and immediately destroying the original using a cross-cut shredder, incinerated, or pulped or detaching and immediately destroying using a cross-cut shredder, incinerated, or pulped. See records retention policy below.

b. All systems that print out the credit card number on any receipt or report must print the last four digits of the card number unless there is a demonstrated business need. This includes all university issued credit card terminals.

c. Card information must not be communicated via unencrypted electronic communications (e.g., email, instant messaging, text). Merchants shall not email/instant message, or text card information. If a merchant contacts a customer via email/instant message/text, all card information must be deleted prior to the message being sent. Under no circumstance should departments take a photocopy of a customer's debit or credit card.

d. If you receive an email containing full credit card number or other sensitive data, either in the body of the email or as an attachment (e.g. report), immediately contact your campus e-Commerce representative for instructions on how to handle this communication.

e. Any cardholder data that is stored until processed must be stored securely in a locked cabinet, locked drawer, safe, vault or equivalent level of secure storage (locked) then destroyed using a cross-cut shredder, incinerated, or pulped.

f. After a transaction has been authorized, access to card data should be limited to staff with a sound business need to access this information. All hardcopy Cardholder information should be stored securely in a locked cabinet, locked drawer, safe, vault or equivalent level of secure storage (locked) or destroyed using a cross-cut shredder, incinerated, or pulped. Departments needing to retain sensitive cardholder data

beyond transaction authorization must submit a request to the Amherst campus Controller indicating the following:

1. Explanation of the business need to retain credit card data
2. Length of time data will be retained, i.e. X days beyond transaction date
3. Method to secure printed credit card data which must include suitably locked file cabinets etc.
4. Description of who can access stored information
5. Method by which data will be destroyed

4. Record Retention and Disposal Guidelines for Credit Card Transactions

   a. Departments must retain the invoice or other relevant information pertaining to a sales transaction for 3 years after the transaction date.

   b. After the retention period has lapsed, departments must dispose of records using cross-cut shredder, incinerated, or pulped to ensure sensitive customer data is not compromised.

   c. Archived documents containing full payment card numbers should be identified, stored securely in a locked cabinet, locked drawer, safe, vault or equivalent level of secure storage (locked), and properly disposed of after the retention period has lapsed.

   d. An inventory of stored credit card data is required at a minimum annually and an inventory log or other record of media inventory activities must be maintained.

5. Third Party Applications

   a. CyberSource has been identified as the third party processing vendor of choice for all web-based e-commerce activity and compliance with PCI standards is handled by the President's Office

   b. The use of any other third party credit card processor must be approved by the e-commerce representative and Treasurer's office

   c. All third party credit card processing vendors are subject to PCI compliance standards including quarterly network scans by approved vendors, completion of annual self assessment questionnaires, listing on VISA's list of compliant service providers and other compliance requirements.

   d. All new contracts with third party or outside vendors must contain language requiring the vendor be PCI DSS Compliant and will remain PCI DSS -Compliant.

   e. All new credit card processing with a third party vendor is potentially subject to a Qualified Security Assessor review at the expense of the department

   f. Schools and departments will be responsible for all fines and penalties relating to loss or theft of credit card data from third party vendors.

   Questions concerning these policies may be forwarded to the Controller's Office at 545-0806.