



UNIVERSITY OF MASSACHUSETTS
TREASURER'S OFFICE

Treasurer's Fiscal Procedure No. 08-01
Effective Date: March 1, 2008

Fiscal Procedure – E-Commerce

Operational

- Credit card terminals must be batched out daily.
- Campus merchants (departments) may not store in any form the magnetic strip, which consists of track data, CVV2 data or PIN data.
- Campus merchants (departments) may not store in any manner the 16 digit credit card number of the customer.
- If your system automatically generates a receipt which displays the card number, the first 12 digits must be defaced with permanent marker. If your electronic system is storing the full 16 digits of the credit card, your system must be modified to comply with the new standards. In the instance where business practices require the retention of the full 16 digit credit card number, the exception must be documented and a plan to eliminate the exception by June 30, 2008 must be in place. All exceptions must be approved by both the University Treasurer's Office and the Campus Vice Chancellor for A&F.
- The detail batch report produced by the point-of-sale terminals prints the full account number. This report should not be run if it is not required. The report must be destroyed as soon as it is no longer needed. If it is kept it must be stored in accordance with PCI standards.
- All requests for credit card receipt copies and chargebacks must be processed immediately. Failure to respond before the deadline will result in the chargeback being processed by the card company. Credit card copies must have the first 12 digits of the account number defaced with permanent marker prior to transmission.
- University Records Retention Policy states that we must retain all credit card receipts for three years. PCI Standards also require that these records be classified by labeling as "Confidential" and stored securely. At the end of three years they must be properly disposed of by being cross-cut shredded, incinerated or pulped.
- All credits specific to CyberSource applications must be processed online through the University Treasurer's Office within 60 days of the original transaction and are based on a transaction reference number. Card number is not required. Beyond 60 days, credits must be processed manually by the receiving site.
- To process a credit for a point-of-sale terminal, ideally you should have the card present and swipe it through the terminal. If the card is not present then there should be communication with the cardholder to get the full number to be used to enter into the terminal. There should not be storage of full card numbers.

Inventory

- Each campus must maintain a complete and accurate inventory of all credit card processing locations as well as documentation regarding third party vendors contracted to process credit cards. Process flows and technology configuration should be documented and updated as needed.
- Campus E-commerce representatives must be involved in and approve any decisions to accept credit cards or other electronic form of cash receipts.

PCI Compliance

- Campus E-commerce representatives and Campus Bursars will work with departments to provide the necessary guidance in the areas of PCI Compliance, internal controls, deposit techniques and reconciliation.
- CyberSource has been identified as the third party vendor of choice for all e-commerce activity. Any deviation from the use of CyberSource must be approved by your campus Vice Chancellor for A&F as well as the E-commerce Committee. All third party vendors are subject to the same standards for data compliance and security. Proof of PCI compliance must be provided on an ongoing basis. Proof will be provided no less than annually.
- E-commerce representatives have the authority to shut down a merchant who is not in compliance with University of Massachusetts PCI Standards.
- Failure to follow the newly approved standards for credit card merchants subjects the University to fines and penalties. Any fines will be the responsibility of the campus.
- All broken and discontinued POS terminals must be returned in a secure manner to the University Treasurer's Office for disposal.
- Use of any unauthorized third party credit card processing vendors must be immediately terminated.
- All new payment applications must be listed on Visa List of Validated Payment Applications. If the application is not listed the campus must demonstrate that the application was developed under PABP guidelines and that their environment is PCI Compliant. The campus must provide the University Treasurer's Office with a PABP Implementation Guide to help ensure that once the application is implemented it is in compliance.
- All charge card applications written in-house must be developed using VISA's PABP, Payment Application Best Practices and validated to be PCI Compliant before going live.

Third Party Applications

- All third party credit card processing vendors are subject to PCI Compliance Standards. In addition they are subject to quarterly network scans that must be performed by an approved scanning vendor. The completion of annual self assessment questionnaires is also required. It is the responsibility of the campus to monitor and maintain current documentation.
- Outside (third party) vendors must be listed on Visa's List of Compliant Service Providers or if not listed, they need to submit a certificate to the campus stating that they are PCI Compliant, and the date specific to that compliance. This document must be updated annually.
- All new contracts with third party or outside vendors must contain language requiring that the vendor be PCI Compliant and they will remain PCI Compliant. Failure to do so gives the University the right to terminate the contract at no penalty to the University of Massachusetts.
- All new contracts with third party or outside vendors must contain language that the vendor acknowledges that they are responsible for the security of cardholder data that they possess.