1. Introduction

Debit and Credit Card Receipt Standards apply to the administration of accepting debit and credit cards as payment for goods and services. Campuses may establish guidelines within the scope of University policy regarding merchant debit and credit card receipts. Guidelines may be more, but not less, restrictive than the Treasurer’s Administrative Standards.

Purpose
To reduce the risk of debit and credit card fraud, protect University resources and to ensure cardholder data is private and secure.

Scope
This standard applies to all approved University of Massachusetts merchants, including employees, contractors, and managers, who are responsible for accepting payments, reconciling reports, providing technical support, or securing equipment used to transact debit and credit card payments.
2. Fiscal Standards for Debit and Credit Card Receipts – Table of Contents

A. PCI DSS
B. Acceptable Credit Cards
C. Security & Technical Standards
D. Training & Annual Compliance
E. Opening a Merchant Account
F. Storage & Access to Cardholder Data
G. Methods of Processing Transactions
   • Point of Sale (POS) terminal – Analog
   • Point of Sale (POS) terminal – Wireless
   • Online Payment Gateway
   • Mobile Card Reader
   • Payment Application
H. Requirements of Campus e-Commerce Representatives
I. Requirements for Any Individual Involved With Card Processing
J. Third Party Applications
K. Posting Debit and Credit Card Transactions and Fees to General Ledger
L. Processing Refunds & Chargebacks
M. Discarding Equipment
N. Closing a Merchant Account
O. Non-Compliance
P. Incident Response
Q. Related Links
Section A. PCI DSS
The Payment Card Industry Security Standards Council, or PCI SSC, was formed in 2006 as an open global forum to develop, maintain and manage PCI Security Standards, including the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements.

The Council is comprised of five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Each of these payment brands recognizes the PCI DSS as the technical requirements for their data security compliance programs. Each also recognizes Qualified Security Assessors and Approved Scanning Vendors certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

The University provides proof of compliance on an annual basis by filing a PCI DSS Self-Assessment Questionnaire to its acquiring financial institution. The PCI DSS SAQ is a validation tool consisting of two components: (1) Requirements to comply with PCI DSS standards and (2) a Validation of Compliance whereby merchants verify and demonstrate their compliance status.

Compliance to PCI DSS standards is mandatory. Each merchant is responsible for providing proof of compliance on an annual basis, running quarterly security scans on all relevant IP addresses and for maintaining compliance throughout the year. All documents and notices of non-compliant situations should be forwarded to the appropriate campus eCommerce representative.

Merchant and Campus Responsibilities

- Campus E-commerce representatives and Campus Bursars will work with merchants to provide the necessary guidance in the areas of PCI Compliance, internal controls (including restricting access to cardholder data), deposit techniques and reconciliation.
- E-commerce representatives have the authority to suspend the account of a merchant who is not in compliance with the University of Massachusetts Fiscal Standard and Procedure – E-Commerce and PCI.
- Failure to follow the PCI DSS standards for credit card merchants subjects the University to fines and penalties. Any fines will be the responsibility of the campus.
- Use of any unauthorized or non-compliant third party credit card processing vendors must be immediately terminated.
- Any merchant accepting credit card payments in any format is required to complete the appropriate PCI SAQ (Self-Assessment Questionnaire) annually.
- Transmission of quarterly scan results and the annual SAQ will be sent and tracked by the Treasurer’s Office to the acquiring bank.

Section B. Acceptable Credit Cards
The University currently accepts VISA, MasterCard, Discover and American Express. All Merchants should follow the card acceptance guidance for each card brand.
Section C. Security & Technical Standards
PCI DSS applies to the security of transactions related to all credit card brands as well as all system components. A system component is defined as any network component, server, or application that is included in or connected to the Cardholder Data Environment. The Cardholder Data Environment is that part of the network that possesses cardholder data or sensitive authentication data.

The University has a Written Information Security Plan. The WISP sets forth University procedures for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting University information assets and technology resources. The WISP framework and security programs apply to all University locations. The security program is administered by the UMASS Information Security Council. All merchants should adhere to the WISP and be aware of University policy regarding PCI DSS.

In order to ensure on-going compliance, merchants shall adhere to the following:

Primary Account Number (PAN)

- Campus merchants may not store in any manner full 16 digit credit card numbers (PAN).
- Unprotected PAN should not be sent via end-user messaging technologies including but not limited to email, instant messaging, text message, or social media.
- Electronic records containing cardholder data should not contain the full PAN. If you receive a report containing the full PAN please contact your campus eCommerce representative immediately for instructions on permanently deleting the file.

Section D. Training and Annual Compliance
Merchants are responsible for the security of cardholder data (CHD). The University maintains a web-based Security Awareness Training program. Any person who has access to CHD must complete annual PCI Awareness training and comply with PCI DSS and University requirements associated with the handling of CHD.

- Campus eCommerce representatives are responsible for maintaining a current list of all individuals who meet the standards for PCI Awareness training.
- Individuals who have access to cardholder data must complete annual PCI Awareness training. Failure to complete annual training will result in the loss of access to merchant sites and the cardholder data environment until training is completed.

Section E. Opening a Merchant Account
Prior to entering into a contract for services or purchasing hardware or software, an entity desiring to accept debit/credit card payments must obtain written approval from their campus eCommerce representative and must provide all required New Merchant documentation. The merchant is responsible for all bank fees associated with opening and maintaining a merchant ID, the cost of any equipment and supplies necessary to process transactions, and for all expenses associated with proving and maintaining compliance. Bank and merchant accounts may only be opened by the University Treasurer’s Office. Any account that has not been opened and approved by the University Treasurer’s Office must be closed immediately.
All new merchants must prove compliance prior to processing a “live” transaction.

New merchant request forms can be found on the University Treasurer’s Office Merchant Services link:  http://www.umassp.edu/treasurer/cash-management/merchant-services

Section F. Storage and Access to Cardholder Data (CHD)

- Merchants may not store in any form the magnetic stripe track data, CVV values or PIN data.
- Under no circumstances should merchants take a photocopy of a debit or credit card.
- After a transaction has been authorized access to CHD should be limited to staff with a business need to access this information.
- Credit card receipts should be stored for the period of time identified by University or Campus Records Retention Policy. These records should be classified “Confidential” by labeling and storing securely. Receipts should not contain the full PAN. PAN data should be rendered illegible by redacting the data on the original document and storing a copy of that document. The original document should be immediately and properly disposed of. At the end of the retention period documents must be properly disposed of by being cross-cut shredded, incinerated, or pulped. Containers storing documents to be destroyed should have a lock preventing access to its contents.
- Forms used for processing card payments should include card data at the bottom of the page so that it can be easily removed from the form and properly destroyed.

Section G. Methods of Processing Transactions
The University accepts payments via analog POS Terminals, Wireless POS Terminals, On-Line Payment Gateway, QR Code, Mobile Device and Mobile Applications. Use of any of these methods must be approved by the campus eCommerce representative and must be compliant when made operational. Emerging technologies will be reviewed by the eCommerce group and new methods may be added.

Lists of approved terminals, devices, and software can be found on the University Treasurer’s Office Merchant Services link:  http://www.umassp.edu/treasurer/cash-management/merchant-services

POS & Wireless POS Terminals

- Merchants are responsible for ensuring they only use PCI compliant POS terminals and must replace any non-compliant or obsolete terminals at their own expense.
- POS terminals should only be used on campus. If a business need arises to take the terminal off campus merchants must obtain approval from their campus eCommerce Representative prior to taking a terminal off campus. The requesting merchant must confirm the connection type that will be used at the outside venue is secure and falls within PCI Compliance guidelines. The merchant must also agree to monitor the terminal at all times and keep it securely locked when not in use, in keeping with PCI Compliance guidelines.
On-Line Payment Gateway & Third Party Vendors

- The University has identified third party vendors of choice for all online activity. Any deviation from the use of these vendors must be approved by the 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. A list of approved third party vendors can be found at: [http://www.umassp.edu/treasurer/cash-management/merchant-services](http://www.umassp.edu/treasurer/cash-management/merchant-services)

- Any merchant processing online credit card payments must work with their campus IT Security Department to determine if they will need to complete and submit quarterly scans.

- Outside (third party) vendors must be listed on the PCI list of Validated Payment Applications or if not listed, they need to submit documentation from an approved QSA acknowledging 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 throughout the term of the contract. If the third party vendor is not the payment processor, their contract language must state that they will only use a PCI compliant payment processor throughout the term of the contract. Failure to do so gives the University the right to terminate the contract at no penalty to the University of Massachusetts. The required language can be found at: [http://www.umassp.edu/treasurer/cash-management/merchant-services](http://www.umassp.edu/treasurer/cash-management/merchant-services)

- 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.

Mobile Device

- Merchants should use only University owned or provided devices. Merchants should not use their own personal device.

- eReaders attached to mobile devices must use P2PE software as a best practice.

- Technical requirements and instructions for device configuration can be found at: [http://www.umassp.edu/treasurer/cash-management/merchant-services](http://www.umassp.edu/treasurer/cash-management/merchant-services)

Section H. Requirements of eCommerce Representatives

- Campus E-commerce representatives must be involved in and approve any decisions to accept credit cards or other electronic form of cash receipts.

- Campus E-commerce representatives and Campus Bursars will work with merchants to provide the necessary guidance in the areas of PCI Compliance, internal controls (including restricting access to cardholder data), deposit techniques and reconciliation.

- Each campus shall maintain an inventory of all outsourced vendors that process card payments. This inventory should include process flows and technology configuration and should be updated as needed. Proof of their PCI compliance should be provided no less than annually.

- All third party credit card processing vendors are subject to PCI DSS Standards. In addition they may be subject to quarterly network scans that must be performed by an Approved Scanning Vendor (ASV). The completion of annual self-assessment questionnaires is required. It is the responsibility of the campus to monitor and maintain current documentation.
• Campuses are responsible for ensuring that third party vendors remain PCI compliant throughout the term of the contract.

• E-commerce representatives have the authority to suspend the account of a merchant who is not in compliance with the University of Massachusetts Policy and Standards for Merchant Debit and Credit Card Receipts.

• Use of any unauthorized or non-compliant third party credit card processing vendors must be immediately terminated.

Section I. Requirements of Any Individual Involved With Card Processing
Employees, managers, or contractors who accept payment or who have access to cardholder data at or on behalf of the University must complete PCI Security Awareness training on an annual basis.

Section J. Third Party Applications
• New third party installations must be reviewed by a QSA (Qualified Security Assessor) prior to accepting payments. The QSA deliverable should be a written report stating that the installation was installed in a PCI compliant manner. Additionally, campuses should periodically review these installations to confirm ongoing compliance. On-going monitoring or review of insignificant changes to existing merchants may be performed by an Internal Security Assessor (ISA).

• All new payment applications must be listed on the PCI list of Validated Payment Applications. If the application is not yet listed, 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. This will demonstrate that the application was developed under PABP guidelines and that their environment is PCI compliant.

• All payment card applications written in house must be developed using VISA’s PABP, Payment Application Best Practices and validated to be PCI compliant before being made operational.

Section K. Posting Debit and Credit Card Transactions and Fees to General Ledger
• Debit and credit card revenue is posted to the General Ledger (GL) via an interface. Merchants should not post entries directly to record revenue. Access to system reports is granted through campus IT Security roles and is based on a proven business need. A crosswalk of merchant Id to GL chartfield information is maintained by the University Treasurer’s Office. Merchants should notify the Treasurer’s Office immediately upon determining any variances in their daily “bank to book” reconciliation.

• Fees related to debit and credit card transactions are posted monthly by the University Treasurer’s Office and are charged to the merchant.
Section L. Processing Refunds and Chargebacks

- 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 mask all but the first six and last four digits of the account number (PAN) prior to transmission.
- To process a credit for a point-of-sale terminal, the card should be presented and swiped 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 in any format.
- 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 can be processed manually by the receiving site or as a stand-alone credit through the Treasurer’s Office.

Section M. Discarding Equipment

- All out-of-warranty, broken, and discontinued POS terminals must be returned in a secure manner to the University Treasurer’s Office for disposal.
- POS terminals still under warranty may be returned directly to the vendor for a replacement terminal. In order to maintain an accurate inventory, the Treasurer’s Office should be notified of the serial number of the terminal to be returned and the serial number of the replacement terminal.
- Merchants should clear the memory of POS terminals should before returning them for disposal or replacement.

Detailed procedures on terminals under warranty, clearing memory, and shipping addresses, can be found at: http://www.umassp.edu/treasurer/cash-management/merchant-services

Section N. Closing a Merchant Account
Merchants should notify their campus eCommerce representative to request an account closure.

Section O. Non-Compliance
Ecommerce representatives, in coordination with the Treasurer’s Office, have the authority to shut down a merchant who is not in compliance with University of Massachusetts PCI Standards. If a merchant or service provider does not comply with the PCI DSS or fails to rectify a security issue, they may be subject to fines by the Card brands, (Visa, MasterCard, American Express, Discover), or their use of Card processing may be restricted. Fines and penalties arising from a merchant’s failure to follow or comply with the PCI DSS are the responsibility of the violating campus.
Section P. Incident Response
In 2007 Massachusetts State Law (Chapter 93H) went into effect requiring disclosure in the event of:

- Unauthorized acquisition or unauthorized use of unencrypted personal data or,
- Encrypted electronic personal data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by an agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. This law applies to and defines personal information as a resident’s first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

  (a) Social Security number;
  (b) Driver's license number or state-issued identification card number; or
  (c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account.

If a merchant is aware of or suspects a security breach of Card numbers, the campus eCommerce representative should be notified immediately.

Section Q. Related Links
- University Policies & Guidelines on Data Computing: http://www.umassp.edu/bot/policies
- PCI Security Standards Council: https://www.pcisecuritystandards.org/
- Treasurer’s Fiscal Standard No. 08-01 Merchant Debit & Credit Card Receipts: http://www.umassp.edu/treasurer/cash-management/merchant-services