University of Massachusetts
Amherst • Boston • Dartmouth • Lowell • Medical School • UMassOnline

University Treasurer's Office

Treasurer's Fiscal Procedure No. 08-01
Revised: December 2011
Revised: February 2015

Treasurer's Fiscal Procedure No. 08-01
Effective Date: March 1, 2008
Merchant Debit and Credit Card Receipts

Purpose
This Fiscal Standard has been developed and revised to establish a framework for accepting debit and credit card payments in any manner at any campus or affiliated University entity. The University of Massachusetts requires any department that accepts credit cards do so in a manner that is compliant with industry standards, including Payment Card Industry Data Security Standards (PCI DSS), and in accordance with the procedures and the document titled Treasurer's Administrative Standards for Merchants Accepting Debit & Credit Card Payments.

Introduction
The University supports the acceptance of debit and credit cards as payment for goods and services to improve customer service and bring efficiencies to cash collection processes. This standard applies to any approved University of Massachusetts merchant accepting payment via debit or credit card. Campus guidelines and procedures may be more, but not less, restrictive than the Standards for Merchants Accepting Debit & Credit Card Payments. All guidelines and procedures must follow the security standards dictated in the Payment Card Industry Data Security Standards (PCI DSS) and the University's Written Information Security Plan (WISP).

Fiscal Standard Statement
This standard pertains to all employees, managers, or contractors accepting payments or who have access to cardholder data at or on behalf of the University of Massachusetts.

- Campus e-commerce representatives are responsible for disseminating all relevant policies, standards and guidelines to ensure merchants are knowledgeable in PCI DSS requirements and Incident Management.

- Campus e-commerce representatives will work to ensure that payment software and gateways are installed in a compliant, consistent, and efficient manner with a goal of limiting the number of installations across the University; especially for similar uses.

- A merchant is defined as an entity, department, or unit within a department that accepts payment cards as payment for goods and/or services.

- Homegrown payment applications are required to meet the same PABP requirements as third party applications and should be limited in use.

- A department / group desiring to accept debit/credit card payments via a Point-of-Sale (POS) terminal or mobile device must obtain advance approval from their campus e-commerce representative. Upon approval, the campus e-commerce representative will request a merchant account and purchase of appropriate equipment through the University Treasurer's Office.

- A department / group desiring to accept debit/credit card payments via an online payment gateway must obtain advance approval from their campus e-commerce representative. Upon approval, the campus e-commerce representative will request a merchant account from the University Treasurer's Office.

- All approved merchants must annually prove compliance with PCI DSS and must remain compliant throughout the year. Annual compliance requires submission of a passing Self-Assessment Questionnaire (SAQ), PCI DSS Awareness training, and when appropriate, passing quarterly scans. Merchants who fail to maintain compliance at any time during the year must report the out-of-compliance status to their campus e-commerce representative upon learning of the status.

- Merchants are responsible for the cost of proving and remaining compliant. They are also responsible for all fees, software, and hardware expenses associated with card payments.

- Merchants are responsible for the security of cardholder data (CHD). 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 e-commerce representatives are responsible for maintaining a current list of all individuals who meet the standards for PCI Awareness Training.

- Payments by debit and credit card may be accepted by an approved vendor via an analog POS terminal, Wireless POS terminal, Online Payment Gateway, QR Code, Mobile Device or Mobile Application. Use of any of these methods must be approved by the e-commerce group and must be compliant at the time of installation. Emerging technologies will be reviewed by the e-commerce group and new methods may be added. The guidelines to use any of these methods are addressed in the Standards for Merchants Accepting Debit & Credit Card Payments.

- Security of Cardholder Data (CHD) and the Cardholder Data Environment (CDE) is described in the University's Written Information Security Plan (WISP). All merchants are required to adhere to the WISP and be aware of University policy regarding PCI DSS.

- Campus e-commerce representatives are responsible for ensuring that any vendor accepting or processing debit or credit card payments on behalf of the University are PCI DSS Compliant. The representatives are also responsible for maintaining a list of these vendors and requiring proof of on-going PCI DSS Compliance.

Related Documents

- PCI Security Standards Council: https://www.pcisecuritystandards.org/

- Treasurer's Administrative Standards for Merchants Accepting Debit & Credit Card Payments: http://www.umassp.edu/treasurer/cash-management/merchant-services