

<b>Subject: Credit Card Merchants</b>	Author: Controller’s Office/Treasury Dept.
Effective Date: February 1, 2010	Last Review Date:
Last Revision:	Revised By:
Contact Name: David M. Woods	Contact Email: <a href="mailto:treasmgt@louisville.edu">treasmgt@louisville.edu</a>
Approved By: Larry Zink	Page 1 of 5

## Purpose

In order to ensure that credit card activities are consistent, efficient and secure, the University has adopted the following policy and supporting procedures for all types of credit card activity transacted, whether in-person, over the phone, via fax, mail or the Internet. This policy provides guidance so that credit card acceptance complies with Payment Card Industry Data Security Standards (PCI DSS). Please visit [PCI DSS](#) and/or PCI DSS – [Questions and Answers](#) for additional details.

## Policy

### Applicability

Any University employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card payments for the University, is subject to adherence to this policy. Failure to comply may result in disciplinary actions for any involved employee (in accordance with Human Resources Policies and Procedures), termination of a contract with a contractor or agent, or loss of a department’s credit card acceptance privileges.

### Merchant Department

Any department accepting credit card payments on behalf of the University for gifts, goods, or services, (the “Merchant”), shall designate an individual within their department who shall have primary authority and responsibility for credit card transaction processing. This individual shall be referred to as the Merchant Department Responsible Person or “MDRP”.

All MDRP’s shall:

- 1) Execute on behalf of the department the process to create a Merchant Account ([Application for a New Merchant Account](#)).
- 2) Ensure that all credit card data collected by the Merchant Department in the course of performing University business, regardless of how the payment card data is stored, is secured by adhering to the following:
  - All systems that process credit cards require approval by Treasury Management with consultancy from Information Technology.
  - Departments must contact Treasury Management before entering into any contracts with service providers or third party vendor for software and/or equipment related to credit card processing.
  - If a Virtual Terminal product is used as the method of processing, a dedicated workstation is required whose *internet access is limited to credit card processing only*.

A custom Firewall must be installed for the workstation by the University's Information Technology department. While the University has a global firewall protecting Merchants, to an extent, from threats outside the University, an additional firewall is needed to protect from attacks inside the University. A one-time setup fee and annual fees will be incurred with this method. Current pricing can be found on the [Application for a New Merchant Account](#).

- If a Credit Card Terminal Swipe Machine is used a dedicated phone/fax line is required.
- Departments who are not approved for a Merchant Account may qualify to [submit credit card payment transactions to Bursar for processing](#).
- All dedicated computers that process credit cards must use a desktop. If a laptop dedicated to credit card processing must be used, wireless capability must be disabled.
- Departments must not maintain sensitive credit card data such as credit card numbers, card type, expiration date, PIN, card validation codes and/or any magnetic strip data.
  - Credit card or personal payment information shall never be downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
  - The three digit card validation code (CVV2, CVC2, CID) printed on the signature panel of a credit card and/or any magnetic strip data shall never be stored in any form.
  - If it is necessary to display credit card data, all digits except the last four digits of any credit card account number shall always be masked.
  - If it is necessary to maintain physical records, documents containing credit card and/or personal payment data shall be securely stored in a locked file cabinet.
  - All physical and electronic credit card and personal payment data that is no longer deemed necessary or appropriate to store must be properly destroyed or rendered unreadable.
- Each department maintaining a Merchant Account must complete an annual self assessment questionnaire.

No University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting business on behalf of the University may sell, purchase, provide or exchange said information in any form to any third party other than to the University's merchant card processor, depository bank, VISA, MasterCard, or other credit card company, or pursuant to a government request. This includes, but is not limited to, imprinted sales slips, photo or carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction. All requests to provide information to a party outside of the department shall be coordinated with Treasury Management.

### **Payment Card Industry Data Security Standards (PCI DSS) Compliance**

All University Merchants must comply with PCI DSS. These standards may be found at the [PCI Security Council website](#).

Annually, every Merchant of the University must submit to Treasury Management a completed PCI DSS Self-Assessment Questionnaire, also known as SAQ ([A, B, C or D](#)). The specific SAQ to use relating to the type of credit card acceptance method will be communicated to each Merchant. Additionally, Merchants will be subject to remote vulnerability network scans, server scans and applications scans performed by the University's Information Technology (IT) department and/or approved third parties.

Additional information may be found at [PCI DSS](#).

## **Procedures**

### Process to Implement Acceptance of Credit Card Payments

- 1) The MDRP shall take the following steps to implement payment card processing at the University:
  - a) Read these procedures thoroughly.
  - b) Complete and sign the [Application for a New Merchant Account](#).
  - c) Forward the application to the VP/Dean or Director/Chair as appropriate.
- 2) It is the responsibility of the VP/Dean or Director/Chair to approve the Application and the designated Merchant Department Responsible Person (MDRP). After verifying all information is correct and signing the Application, the completed signed original must be submitted to Treasury Management.
- 3) Treasury Management is responsible for final review. After the application has been approved, the applicant will be given the appropriate SAQ to complete.
- 4) The responses provided on the SAQ must be approved by the VP/Dean or Director/Chair acting as the Merchant Executive Officer.

### Notification of Change of Merchant Account

Merchants must notify Treasury Management prior to making any changes to their method of processing after the Merchant Account has been initially setup (i.e., changing from terminal based processing to virtual terminal or online acceptance, changes to their business process, DBA name or address) via email to [TREASMGT@louisville.edu](mailto:TREASMGT@louisville.edu). Changes in personnel related to the Merchant account shall be submitted using the [Merchant Account Users Setup](#) form and the responsibility of MDRP to maintain a current status.

### Seasonal Merchant Accounts

A Merchant Account can be setup on or changed to a seasonal basis, for example activated for a period of months and deactivated (suspended) when inactive, thus eliminating the monthly account maintenance fee during the inactive period.

### Termination of Merchant Account

If a Merchant no longer wishes to accept credit cards, the MDRP must notify Treasury Management via email at [TREASMGT@louisville.edu](mailto:TREASMGT@louisville.edu). Any equipment (swipe terminals) associated with the terminated Merchant Account should be returned to Treasury Management for safekeeping. Merchant accounts with no activity after (24) months will be terminated. Be aware an active status account is subject to monthly account maintenance fees by the processor.

### Equipment and Supplies

Equipment for processing credit cards shall be PCI compliant and must be purchased through Treasury Management. Current pricing can be found on the [Application for a New Merchant Account](#).

Equipment decommissioned due to PCI non-compliance must be returned to Treasury Management for disposal.

### Software and e-Commerce

Any department desiring an online web application (e-Commerce) must contact Treasury Management to coordinate web-based 3<sup>rd</sup> party payment solutions with the payment processor under contract with the University. Information Technology can serve as an internal resource for interfacing needs. Coordination between the requesting department, IT and Treasury would occur to facilitate the cost proposal and scheduling process. Initial request should be directed to Treasury Management.

Server-based software applications and point-of-sale (POS) systems (i.e., cash registers, event ticket distribution) that collect and transmit credit card data for payment must be certified as PCI DSS compliant and listed on [VISA's List of Validated Payment Applications](#). Any department interested in implementing a server-based software application or POS system in order to accept credit card payments must notify Treasury Management to ensure PCI DSS compliance.

### Card Association Rules and Regulations

VISA, MasterCard, American Express and Discover are the only credit cards that may be accepted. Merchants are expected to comply with the rules and regulations set forth by each of the card associations in the processing of credit card payments. Each card association's rules and regulations can be found on their company's websites, or you can request a copy from Treasury Management. The card associations may impose fines or revoke the privilege of accepting credit cards for not complying with their rules and regulations. The following card association rules are noteworthy and must not be violated by a University Merchant:

1. No minimum credit card transaction amount may be set.
2. No surcharges to specifically cover the processing costs may be placed on credit card transactions.
3. You must accept a credit card as payment unless the transaction cannot be authorized.
4. If you require additional information, such as a driver's license or phone number, do not record the information on the sales draft.
5. Refunds for purchases made by credit card must be made by crediting the card, not by cash or check.

### Associated Costs

Merchants are responsible for all costs associated with the acceptance of credit cards including costs of supplies and equipment, as well as processing fees (i.e., interchange and per transaction). Merchants are also responsible for responding timely in defense of a chargeback or any credit card transactions that are disputed and charged back to the University.

### Accounting for Transactions

University Accounting will post deposits received for the full amount of the transaction on a daily basis to the Speedtype and Account code designated by the Merchant. Credit card fees are charged and recorded on a monthly basis. Therefore, Merchants do not need to prepare journal entries to post the transactions unless re-allocation is needed via IUT. However, it is the Merchant's responsibility to review the activity and to ensure the data is correct in the enterprise financial system.

### Review of Merchants

Periodic reviews of Merchants will be coordinated by Treasury Management. Additionally, credit card handling procedures are subject to audit by Internal Audit. Merchants not complying

with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.

### Security

Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments.

Departments that accept credit cards are responsible for ensuring all credit card information is received and maintained in a secure manner in accordance with the payment card industry standards. Individual departments will be held accountable if monetary sanctions and/or card acceptance restrictions are imposed as a result of a breach in PCI compliance.

Under no circumstance shall credit card information be obtained or transmitted via email. Credit card information shall not be stored on individual PCs or servers that have not been deemed PCI compliant. All hard-copy credit card information must be stored in a manner that would protect the individual cardholder information from misuse.

Additional information related to security may be obtained at [PCI DSS](#).

### Process for Responding to a Security Incident

In the event that a Merchant knows or suspects that credit card data, including card number and card holder name, has been disclosed to an unauthorized person or stolen, the Merchant shall immediately take the following steps:

1. The MDRP or any individual suspecting a security breach shall immediately contact the Assistant Treasurer, in Treasury Management. If the Assistant Treasurer is unavailable the Controller should be contacted.
2. If an actual breach of credit card data is confirmed, the Assistant Treasurer shall alert the Merchant bank, the UofL Police Department, the Legal Office, the Controller, the Director of Internal Audit, Chief Information Security Officer, the Director of IT and any relevant regulatory agencies of the breach.

### Other Reference Materials

[PCI DSS](#)

[PCI DSS Questions and Answers](#)

[VISA](#)

[MasterCard](#)

[Discover](#)

[American Express](#)

WARNING: Some Web sites, to which these materials provide links for the convenience of users, are not managed by the University of Louisville. The University does not review, control, or take responsibility for the contents of those sites.