UNIVERSITY OF LOUISVILLE

Vice President for Finance
Policy/Procedure

Subject: Credit Card PCI Merchants PROCEDURE	Author: Controller’s Office/Treasury Dept.
Effective Date: February 1, 2010	Last Review Date: March 2015
Last Revision: April 1, 2015	Revised By: Jill Riede
Contact Name: Jill Riede	Contact Email: treasmgt@louisville.edu
Approved By: David Woods/Larry Zink	Page 1 of 3

PROCEDURES STATEMENT: The following procedures are in support of the University’s Credit Card Merchants (PCI) Policy.

APPLIABILITY OF PROCEDURES: Any University employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance or processing of credit card payments for the University, is subject to adherence to these procedures.

PROCEDURES:

Merchant Department Responsible Person (MDRP)

Any department accepting credit card payments on behalf of the University for gifts, goods, or services, (the “merchant”), shall designate an individual(s) 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 MDRPs shall be responsible for the following:

Merchant Creation

MDRP shall take the following steps to create a merchant account to accept card payments at the University:

1. Read Credit Card (PCI) Policy and these procedures thoroughly.
2. Complete and sign the Application for a New Merchant Account.
3. Submit signed application to Treasury Management.

Change of Merchant Account Notification

Merchants must notify Treasury Management via email at TREASMGT@louisville.edu prior to making any changes to their merchant account which include: business name change, business process changes, personnel changes, address change and contract changes. It is the responsibility of the MDRP to maintain current account information.

Seasonal Merchant Accounts

Upon notification to Treasury Management, a merchant account can be changed to ‘seasonal status’ by ‘deactivating’ and ‘reactivating’ merchant status. This status period must be at least (6) months. For example, an annual conference that only needs to be active for a few months, thus eliminating monthly fees 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. Any equipment (swipe terminals) no longer used or decommissioned due to PCI non-compliance must be disposed of following the University's surplus and security policy and standards. Be aware an active status account is subject to monthly account maintenance fees by the processor.

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, unless specific eligibility requirements are met (excludes face-to-face 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 processed on the same card number, not by disbursing cash or a 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, authorization, monthly) and annual PCI allocation costs. 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.

Transaction Accounting

All credit card transactions should be settled daily to ensure prompt payment. Any transactions not settled within 48 hours sustain higher processing fees. University Accounting will post deposits received for the full amount of the transaction on a daily basis to the Speedtype and Account code designated on the merchant application. 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 UA payment grid or IUT. However, it is the merchant's responsibility to review the activity and to ensure the data is correct in the enterprise financial system.

Retrieval Requests & Chargebacks

- A retrieval request most often occurs when a cardholder loses their receipt, does not remember the transaction or questions the transaction for any reason. Retrievals can be requested by the cardholder's bank for up to 18 months from the sale date, therefore, it is crucial that you keep your receipts for this time frame.

- A chargeback occurs when a cardholder or issuing bank disputes a transaction, up to 120 days for most disputes, when one party feels that the merchant has done something in error upon accepting the item. Reasons include: fraud, dispute over merchandise quality, or failure to receive merchandise. The merchant's account is debited and the merchant must provide proof that the transaction is valid and satisfactory to the rules/regulations of Visa/MasterCard to get money back. If contacted directly by the cardholder to resolve a dispute, you can avoid costly fees and processing costs as well as promote goodwill with your customer. If the cardholder does not contact you, respond to inquiries from Merchant Services with as much information as possible about the sales transaction in question.

Merchant Reviews

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.

Incident Response Plan

Merchant/Department Level: 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 contact the Merchant Services Manager, in Treasury Management and the Information Security Office.

Treasury Management Level: If an actual breach of credit card data is confirmed, the Merchant Services Manager 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.

Additional information related to PCI security may be obtained at PCI DSS. For information regarding the University's general Information Security Office Policies please visit the Information Security Office website.