Subject: Credit Card PCI Merchants POLICY	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 4

BACKGROUND: Due to growing consumer concerns over compromised credit card data, the five major credit card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa) joined forces to establish a security program for merchants called the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS is a compliance initiative that dictates security standards for merchants and service providers for the safe handling of credit card information. As a merchant, the University of Louisville has an obligation to protect payment card data. All departments (department(s) refers to College, School, Division, (CSD) throughout document) accepting credit cards, including debit and stored value displaying brand logos, must be familiar with the risks, fees, security requirements and responsibilities involved with being a merchant. The card industry may refuse to allow a department or the University as a whole, to process credit cards and/or levy hefty fees and fines for noncompliance. **Therefore, every UofL department that accepts credit cards must become and remain PCI DSS compliant.**

PURPOSE: 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). PCI DSS standards may be found at the PCI Security Council website. Please visit PCI DSS and/or PCI DSS – Questions and Answers for additional details.

POLICY STATEMENT: Statement: The following policy supplements the University's Information Security policies and supports and provides guidance for compliance with the PCI Security Standards Council standards.

Departments that accept credit cards are responsible for ensuring all credit card information is received and maintained in a secure manner in accordance with University policy and 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.

APPLICABILITY OF POLICY: Any University employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the processing 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, loss of a department's

credit card acceptance privileges, and recognizes that the financial liability, including fines and penalties for a breach, is accepted by the merchant should a breach occur due to negligence of the department to adhere to the University's policies and procedures for Credit Card Merchants.

STANDARDS: Any department accepting credit card payments on behalf of the University for gifts, goods, or services, (the "merchant"), shall be responsible for adhering to the following standards:

1. **Each merchant shall designate an individual(s) within their department who shall have primary authority and responsibility for credit card transaction processing and must conform to a segregation of duties methodology.**

2. **All merchant accounts must be requested through the University's Treasury Management Office as per the** University Credit Card Procedures

3. **Card Data security is the responsibility of all persons involved in the credit card process.**
   - Merchants must not maintain sensitive credit card data such as credit card numbers, 3 digit security code, expiration date, PIN, card validation codes and/or any magnetic strip data.
     - Credit card information shall not be stored on individual desktops, laptops or servers that have not been deemed PCI compliant and approved by Treasury Management.
     - 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.
     - If it is necessary to display credit card data, only the first six digits and last four digits of any credit card account number shall be viewed.
     - 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 and an access log maintained.
     - All physical credit card and personal payment data that is no longer deemed necessary or appropriate to store must be properly destroyed using the University contracted disposal company or a cross-cut shredder.
     - Destruction of electronic credit card data must be done in accordance with PCI standards requiring total eradication of data.
   - All remote access, internally or externally, into the cardholder environment must be reviewed and approved by Treasury Management and Enterprise Security including any additional requirements such as two-factor authentication are required.
   - Under no circumstances should credit card information be obtained or transmitted via email or campus mail.
   - If a fax machine is used to receive payment transactions it must be located in a secure area, not available to the public or unauthorized staff members. Incoming faxes should be removed as they are received and either processed immediately or stored securely until the transaction can be processed. Unless the machine is in a locked office without after-hours access, including maintenance & cleaning personnel, it should be active only during business hours. Therefore, fax machines, under these conditions, receiving card transactions should be turned off at the close of business and on weekend & holidays.

4. Merchant Responsibility

- Development of departmental policy & procedures in support of the University's PCI Policy, including, but not limited to the following: PCIdepttemplate.doc
  - Credit card acceptance process.
  - Incident Response Plan documenting the responsibility & communication in the event of a credit card incident or breach.
  - Card data flow and card device diagram.
- Any individual that is involved with the credit card process will need to complete annual PCI Training which attests their understanding of, and responsibility for, card data security.
- All Merchants of the University must submit an annual Self-Assessment Questionnaire, also known as a SAQ (A, A-EP, B, C, C-VT or D).
- 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. It is the responsibility of the merchant to ensure mitigation of discovered vulnerabilities in accordance with PCI DSS requirements and within stipulated timeframe, if given.

5. Third Party/Service Provider Requirements and Contracts

- Merchants must contact Treasury Management **before** entering into any contracts with Third party service providers for software, payment applications, web hosting services, and/or equipment related to credit card processing.
- All third party service providers must be in compliance with PCI DSS. The department needs to ensure the signed contract for the third party service provider includes the PCI clause, which describes the third party service providers PCI DSS responsibility. A copy of signed contract should be provided to Treasury Management along with proof of PCI DSS compliancy by the third party service provider.
- 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 or depository bank. 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 and the Privacy Office/Information Security.

6. Equipment/Configuration Requirements

- Equipment for processing credit cards must be deemed PCI compliant approved by Treasury Management, configured in accordance with the University's PCI configuration standards and located within the PCI segmented environment.
- Stand-alone terminals must be approved and purchased through Treasury Management.
- Stand-alone 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.
- If a stand-alone terminal is used a dedicated analog telephone/fax line is required. VoIP is not considered PCI compliant. Cellular wireless is compliant. WiFi is not compliant.
- Desktops must be limited to credit card processing ONLY and aligned to meet the University's PCI baseline configuration standards. A custom Firewall must be installed for the workstation by the University's Information Technology department.

- Credit card processing is restricted to dedicated desktops. Exceptions must be approved by the Treasury Office. If an exception approves the use of a laptop, wireless capability must be disabled. This includes all desktop computers provided for student access to pay with a credit card. KVM switches are not allowed for new merchants.
- All credit card swipe devices must be periodically reviewed for tampering.

7. Registration/Payment Forms

Any internal developed registration/payment form(s) utilized by the department must be approved by Treasury Management.

8. Incident Response Plan

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. Verbal contact must occur as leaving a voice mail is not allowed.