Information

Credit Card PCI Merchants

Effective

February 1, 2010

Applicability

This policy applies to all University employees (administrators, faculty, and staff), contractors, and agents.

Administrative Authority

Vice President for Finance and Chief Financial Officer

Responsible Unit

Treasury Management
Office of the Controller
University of Louisville
502.852.8253
treasury@louisville.edu

History

Revision Date(s): April 1, 2015; March 7, 2018; February 10, 2020; February 17, 2022

Reviewed Date(s): March, 2015; March 7, 2018; February 17, 2022

Categories

Reason for Policy:

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.

To ensure that credit card activities are consistent, efficient and secure, the University has adopted this 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).

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.

All University of Louisville departments that accept credit cards must become and remain PCI DSS compliant. 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.

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 standards identified within 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.