LOYOLA UNIVERSITY MARYLAND

— 1852 —

MERCHANT CARD ACCEPTANCE POLICY

DIVISION WITH PRIMARY RESPONSIBILITY: Business and Finance
OFFICE FOR ENSURING COMPLIANCE: Financial Services/Student Administrative Services
CONTACT OFFICE: Student Administrative Services, sas@loyola.edu
EFFECTIVE DATE: April 4, 2017
REVISION HISTORY: N/A
SCHEDULED FOR REVIEW: Annually

POLICY SUMMARY

The Merchant Card Policy (Policy) is intended to establish policy regarding approvals required and practices to be followed by University departments that wish to accept credit card payments.

The Merchant Card Policy supplements the Loyola University Information Security Policy for PCI SAQ C Merchants which is administered by the Office of Technology Services.

REASON FOR POLICY

This policy is necessary to protect our students' and other customers' credit card data, to uphold the University's reputation, to reduce the financial costs associated with a breach of credit card information and to outline required practices for all aspects of processing credit card transactions.

STATEMENT OF POLICY

Documented approval from Student Administrative Services (SAS) is required before any University department may accept Payment Cards and before entering into any contract for purchasing any software or equipment related to Payment Card processing.

Departments that have been approved to accept Payment Cards must implement security requirements, adhere to the standards published and maintained by the Payment Card Industry - Data Security Standard (PCI DSS). The PCI DSS was established by the credit card industry in response to an increase in identity theft and credit card fraud. Every merchant who handles credit card data is responsible for safeguarding that information and can be held liable for security compromises. The PCI DSS has 12 requirements, including controls for handling credit card data, computer and internet security and an annual self-assessment questionnaire. The Loyola University Information Security Policy for PCI SAQ C Merchants is administered by the Office of Technology Services and addresses specific technology safeguards to protect against unauthorized breach of credit card data. All employees are required to attend an initial PCI DSS training session before they are cleared to process transactions. As subsequent training sessions are offer users will be required to attend.

Departments that have been approved to accept Payment Cards must maintain proper business practices as set forth below

All fees associated with Payment Card transaction processing will be paid by the university, but any cost associated with additional software purchased to support the departments initiative will be the responsibility of the department.

The University strategically partners with a third-party vendor to provide a compliant e-commerce application. Campuses, departments or units who believe their needs cannot be met through this partner must request approval from the Vice President for Finance/Administration and Treasurer & Associate Vice President for Technology Services before considering or acquiring third party solutions. Third-party vendors must provide proof of compliance with credit card security standards on an ongoing basis.

Department Responsibilities

Reconciliation
Each department is responsible for the daily close out of Payment Card terminals and reconciliation of activity. All deposits including terminal closeout report and all receipts from the closeout batch are to be submitted within 48 hours to SAS.

Devices/Terminals
Departments must use encrypted terminals issued by the University's Merchant providing bank partner. Departments are required to inspect daily and safeguard all Payment Card devices/terminals and immediately report lost/stolen equipment to SAS, as well as report any device/terminal malfunctions.

Theft/Fraud/Breach
In the event that Cardholder Data is compromised or potentially may be compromised, the department should immediately contact SAS and the Office of the CIO. Compromise includes lost or stolen files with Cardholder Data, electronic loss of data, databases infected with viruses, loss of paper documents with Cardholder Data and any other loss or potential loss, theft or system breach.

Compliance Training
Departments are required to complete annual Security Awareness Training for PCI Compliance offered by Technology Services/Financial Services.

Loyola University employees SHOULD NOT do the following:

- Transmit cardholder's credit card data by e-mail or fax
- Store credit card data for repeat customers on paper in an unsecured area
- Store PIN or CVV2/CVC2/CID number
- Electronically store on the University computer file or server any unencrypted credit card data
- Electronically store any credit card data on laptop or PC's
- Share user IDs for systems access
- Acquire or disclose any cardholder's data without the cardholder's consent

Loyola University employees SHOULD DO the following:

- Store all physical documents containing credit card data in a locked drawer, locked file cabinet, or locked office
- Maintain strict control over the internal and external distribution that contains credit card data
- Change vendor supplied or default passwords
- Properly dispose of any media containing credit card data
- If an unencrypted email is received with credit card data, notify the sender that they should no longer send this information via email and delete the email immediately

- Encrypt Transmission of cardholder data across open & public networks
- Issue all refunds to the original card charged.

DEFINITIONS

Acquiring Bank/Processor
The financial institution that has entered into a contractual arrangement to process Payment Cards for the University.

Merchant(s)
All persons, departments, units and campuses that process, collect, maintain or have access to Payment Card Data.

Merchant Account
A unique account set up with the Acquiring Bank/Processor that provides a department or unit with the ability to process and settle Payment Card transactions for goods, services or donations.

Payment Card
Credit cards, debit cards and some gift/stored-value cards that bear the logo of a card association brand, including but not limited to Visa, MasterCard, Discover or American Express.

Payment Card Data
At a minimum, Payment Card Data consists of the full unique Payment Card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. Payment Card Data may also appear in the form of the unique Payment Card number plus any of the following: cardholder name, expiration date and/or service code.

PCI DSS (Payment Card Industry Data Security Standards)
Security standards developed collaboratively by the major card issuers that must be adopted by all merchants accepting Payment Cards. The standards, which are updated by the Payment Card Industry Security Standards Council, are intended to protect cardholder information from fraudulent use.

CROSS-REFERENCED POLICIES

- Loyola University Information Security Policy for PCI SAQ C Merchants (PCI DSS Compliance Policy)