Saint Louis University
Merchant Card Processing Policy & Procedures

Overview:
Policies and procedures for processing credit card transactions and properly storing credit card data physically and electronically. Saint Louis University must comply with PCI DSS when handling payment card transactions.

Purpose:
To establish a policy for managing merchant accounts and processing credit and debit card transactions to protect the University against the exposure and possible theft of account and personal cardholder information that has been provided to the University, and to comply with PCI DSS requirements. The University must adhere to these standards to limit its liability and continue to process payments using payment cards.

The objectives of this policy are to:

- ensure compliance with PCI DSS and other applicable policies and standards,
- establish the governance structure

I. Payment Card Industry (PCI) Compliance

All University departments that handle, store, process, or transmit cardholder data, including any Saint Louis University employee, contractor, or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit cards and e-commerce payments for the University, must comply with PCI DSS. Saint Louis University has designated Fiserv as the merchant service provider to process credit and debit card payments to the University. As a merchant account holder that accepts payment by credit or debit card, the University must comply with requirements established by PCI DSS

The PCI DSS are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The Council is responsible for managing the security standards, while compliance is enforced by the payment card brands. These standards include controls for handling and restricting credit card information, computer, and internet security, as well as the reporting of a credit card information breach.

A. Annual PCI DSS Self-Assessment

Annually, the SLU PCI Compliance Committee will distribute a questionnaire to assist in completing the annual PCI DSS Self-Assessment. The PCI DSS Self-Assessment is completed annually to prove compliance and applicable standards and policies. Merchants found not in compliance will work with the SLU PCI Compliance Committee to implement appropriate remediation activities.

B. Non-Compliance

Non-compliance and security breaches can result in serious consequences for Saint Louis University, including reputational damage, loss of customers, litigation, and financial costs. Fines and penalties may be imposed on 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.

The Merchant Manager of each University merchant is required to ensure that appropriate controls are implemented and monitored to ensure compliance with this policy. Failure to comply may result in disciplinary actions for any involved employee, termination of employment or contract proioo3.4 37(p)-2 (l)3 (em)4 (e)6 (e t)10euritttit apemrde f Eepart(ity)6 (')3cnitor

II. Types of Cards Accepted

Saint Louis University currently accepts Visa, MasterCard, Discover, and American Express and has negotiated contracts for processing payment card transactions. Individual University business units may not use or negotiate individual contracts with these or other payment card companies or processors. All individual University business units must use the campus negotiated contracts unless otherwise authorized.

This is in an effort to contain costs and compliance to the departments and the University by directing volume to a limited number of card vendors in order to increase our negotiating power for discount rates.

III. Request to Accept Merchant Cards

All University merchant accounts must be authorized by Treasury & Investments and the SLU PCI Compliance Committee. The department must demonstrate a valid business need for a merchant account and demonstrate certain business operation and financial management criteria.

A merchant account is required to accept receipts from credit and debit card transactions. All merchant accounts are created through the University's merchant services provider contract with Fiserv. University merchants must abide by the terms included in this policy as well as the Saint Louis University's Information Security Policies and Standards. To establish a merchant account, or make changes to an existing merchant account, please complete the Merchant Services Account Request/Maintenance Form.

Treasury & Investments will review the Merchant Services Account Request Form and contact the department to assist in the determination of its needs, including but not limited to hardware,

B. Training

Only authorized and properly trained individuals can process credit card transactions and access systems or reports containing credit or debit card data. Employees who have access to cardholder data and/or who are involved in credit card processing must complete credit card security training upon hire and annually. Employees will be notified of their annual training via email. Employees who do not complete the credit card training within 30 days of the initial notification, will have all credit card processing privileges removed and their respective Dean/Vice President will be notified

Contractors, volunteers, and other individuals who are not University employees and who plan to accept or process credit or debit cards on behalf of Saint Louis University, must also be trained prior to taking on their credit and debit card handling duties and annually thereafter. It is the responsibility of the Merchant Manager to notify Treasury & Investments at merchantservices@slu.edu of any non-employees processing or handling credit or debit card data.

Merchant Managers are responsible for ensuring that all individuals who process and handle cardholder data for their merchant location, receive appropriate training. The Merchant Manager is responsible for maintaining a current listing of employees who process or handle credit or debit card data. The employee listing must be submitted to merchantservices@slu.edu quarterly or upon a change in personnel. Merchant Managers are responsible for ensuring new or replacement positions handling or processing credit or debit card data, include the task in the job description and specify on the employee requisition form. The employment requisition form includes an option for the hiring manager to select if the "position" processes or handles credit or debit card data. Treasury & Investments is notified by the Office of Human Resources when these positions are filled so the employee can access and complete training.

V. Merchant Processing Methods or Systems

The University provides departments with secure and convenient methods to process credit and debit card payments. All methods or any alterations of the card processing environment must be approved by Treasury & Investments and the SLU PCI Compliance Committee. Changes include but are not limited to:

- The use of existing merchant accounts for a purpose different from the one specified in the initial Merchant Card Processing Account Request/Maintenance Form.
- The addition or alteration of payment card processing systems, technologies, or channels, and
- The addition or alteration of relationships with third-party payment card service providers.

A. Credit Card Equipment

All credit card equipment is to be requested and approved by Treasury & Investments and the SLU PCI Compliance Committee, including but not limited to POS hardware and software.

- Approval is required before implementing software and installing equipment that processes, transmits, or stores credit card information.
- Departments must inspect their point of sale devices on a regular basis, and should notify Information Security & Compliance and Treasury & Investments if something appears to be changed, added or different. More specifically, departments should inspect for skimming devices or malware that may have been attached to or downloaded onto POS devices, which could be used by thieves to steal credit card information.
- Use of imprint machines to process credit card payments is prohibited, as they display the full 16-digit credit card number and expiration date on the customer copy.

B. Wireless Credit Card Processing

The University provides wireless credit and debit card processing via a University approved First Data or Clover

Third-party vendors are classified into categories. The first category refers to third-party

- Access to computing resources and cardholder data should be limited to only those individuals whose job requires such access. Anyone handling or processing credit or debit card transactions must be first authorized by the department's Merchant Manager.
- Anyone handling or processing credit or debit card transactions must review, and adhere to this policy as well as the Saint Louis University's Information Security Policies and Standards and must protect cardholder information in accordance with PCI DSS.
- Credit or debit card information may be shared only with individuals who have been authorized to access such data by the appropriate Merchant Manager, Dean or Vice President.
- The University discourages sending or receiving credit card information through the mail. Do not collect the 3-digit Card Validation Value or Code (CID/CAV2/CVC2/CVV2] (C 0.00 Td [(d)-( )T

- Completion date of employees PCI Credit Card Security Training
- Upon return of device, Merchant Manager should inspect device per the "Device Inspection Checklist" and indicate on log.

Note: Only cellular devices obtained through Treasury and Investments may be removed from merchant's location unless approved by Treasury and Investments and the PCI Compliance Committee.

- The identity of any third-party persons claiming to be repair or maintenance personnel must be verified prior to granting them access to modify or troubleshoot devices. Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to merchantservices@slu.edu
- The PCI Compliance Committee reserves the right to conduct periodic announced and unannounced device inspections as part of the University's compliance requirements.

C. Processing

- Verify signature of cardholder at the time of transaction and provide a duplicate copy to the cardholder.
- Match payment card's name and signature to cardholder's valid driver's license.
- Verify payment card's expiration date is valid.
- Verify that only the last four digits of the payment card number are printed on the receipt.
- Payment card charges should not exceed transaction amount of purchase.
- The PAN should never be transmitted via any end-user messaging technologies or any other unsecured transmission method such as e-mail, instant messaging, SMS, chat, fax, etc.

D. Refunds

When a good or service is purchased using a payment card and a refund is necessary, the refund must be credited back to the account that was originally charged. Refunds in excess of the original sale amount or cash refunds are prohibited.

All departments must establish a refund policy when processing credit or debit card transactions. The refund policy must be disclosed to your customers, via signs in your physical location, web site or included in mailings.

E. Reconciliation

- Retain and secure merchant copies of receipts until end of day batch settlement.
- Compare each day's credit receipts to daily totals and then group them with the daily batch settlement tape for storage/reference.
- Paper documents containing cardholder data must be processed within two business days of receipt then immediately disposed (see section VII.G).
- Follow Saint Louis University Credit Card Deposit Policy and Procedures for transactions to be credited to department's Workday fund.

F. Disputes and Chargebacks:

A chargeback occurs when a customer has disputed a credit/debit card transaction and the department has either not been able to supply documentation to substantiate the transaction or has not done so on a timely basis. By law, the cardholder has two years to file a dispute. Once a cardholder files a dispute, the issuing bank makes an investigation into the complaint. If the transaction proves to be fraudulent, the bank will refund the original value to the cardholder. If

the merchant does not prove the transaction to be legitimate, the bank will charge back to the merchant the entire value of the transaction along with an additional fee.

Procedures for handling disputes:

- When a customer disputes a transaction, the Merchant and T

Individuals who handle, process, support, or manage payment card transactions. All users must comply with and be informed of PCI DSS and Saint Louis University Merchant Card Processing Policies and Procedures, SLU PCI Supplemental Standard, Saint Louis University Departmental iCard Processing procedures and any associated documents to protect cardholder data. Users must complete PCI Security Training annually and upon hire.

PCI Compliance Committee