Business and Finance Division
SAINT LOUIS UNIVERSITY

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 accepts credit card payments as a convenience to its customers and is committed to protecting and preserving the privacy and security of payment card data collected and processed to conduct University business operations. Saint Louis University has a fiduciary responsibility to patients, students, donors, customers, and payment card processors to comply with the Payment Card Industry Data Security Standards (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 for payment card processing and compliance activities at Saint Louis University,
- define responsibilities for payment card services to various Saint Louis University constituents, and
- provide general guidelines regarding the handling of cardholder data.

Scope:
This policy applies to all University departments, employees, contractors, consultants, or University related organizations, which processes, transmits, or stores cardholder information in a physical or electronic format using University resources. All computers and electronic devices, including wireless devices, involved in processing payment card data are governed by PCI DSS. This includes, but is not limited to; servers, computers, cashiering systems, workstations, and point of sale terminals that process, transmit, or store credit card information.

Policy:
This policy complements and supports Saint Louis University's Information Security Policies and Standards as well as other University policies that protect the University's financial and information technology operations.

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 internal or external parties involved with the acceptance of processing credit cards for payments of goods and services must ensure that PCI DSS compliance is maintained.

The procedures outlined herein are designed to protect cardholder data; maximize the University's compliance with its merchant services provider contract, which includes compliance with PCI DSS and the various credit card brand standards; and to ensure appropriate integration with the University's financial and other systems.

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 with a contractor or agent, and loss of a department's credit card acceptance privileges. Some violations may constitute criminal action.

C. Reporting a Suspected Breach

In the event of a suspected breach of security, including the suspicion that credit card information has been exposed, stolen, or misused, the University merchant must immediately contact the Information Security and Compliance team at 314-977-4000 or e-mail ask@slu.edu.

The Information Security and Compliance team will contact the Treasury team by emailing merchantservices@slu.edu. The Treasury team will then contact the appropriate outside banks.

D. Tools for Assessing Compliance With PCI DSS

The PCI SSC sets the PCI DSS standards, but each card brand has its own program for compliance validation levels and enforcement. University merchants should be familiar with all of the individual credit card brand standards and refer to them periodically. More information about PCI DSS and compliance with specific credit card brands can be found at these links.

- PCI Security Standards https://www.pcisecuritystandards.org
- American Express: www.americanexpress.com/datasecurity
- Discover Financial Svcs: http://www.discovernetwork.com/fraudsecurity/disc.html
- MasterCard Worldwide: http://www.mastercard.com/sdp

- Visa Inc.: http://usa.visa.com/merchants/operations/op_regulations.html

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, software, system requirements, business practices, accounting support, and financial reporting requirements.

The request will then be submitted to the SLU PCI Compliance Committee for final approval. The amount of time required to set-up and activate a merchant account varies based on the nature of the department's business environment, processes, and the extent of involvement by external contractors or consultants. Treasury & Investments will work with the Merchant Manager to ensure the business unit is equipped and operational for merchant processing.

IV. Personnel Requirements

All individuals who have access to cardholder data and/or are involved in credit or debit card processing must meet the following requirements prior to obtaining access.

A. Background Checks

Criminal background checks should be performed for any person prior to assignment of duties that include access to cardholder data or cardholder data environment (CDE).

- Job descriptions for any position with responsibilities that include handling or processing of cardholder data, or maintaining systems that contain cardholder data, must specify that passing a background check is a requirement for the position.
- In cases where a background check returns outstanding issues, the appropriate Merchant Manager must consult Treasury & Investments and those issues will be reviewed with the SLU PCI Compliance Committee, and the Office of Human Resources, to determine whether or not the individual should be permitted to handle cardholder data.

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.

Additionally, employees who have access to cardholder data and/or who are involved in credit card processing must participate in monthly simulated phishing campaigns and cybersecurity training provided by the Information Security Office.

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 swipe terminal over cellular connection. To request a wireless terminal, please complete the Merchant Services Account Request/Maintenance Form.

The University does not permit the use of wireless technology other than the device mentioned above to process or transmit cardholder data. Departments cannot process credit card payments over a wireless internet or cellular connection via laptops, cell phones, tablets, or other similar devices. Any exception to this policy must be requested and approved by Treasury & Investments and the SLU PCI Compliance Committee. If the use of wireless technology is approved, the storage of cardholder data on local hard drives, floppy disks or other external media is prohibited. It is also prohibited to use cut-and-paste and print functions during remote access. Activation of modems for vendors will be permitted only when no other alternative is available and will be immediately deactivated after use.

C. Accepting Credit Card Payments via Phone

The University does not permit the acceptance of credit card payments over the phone. Departments may not receive any credit card information over the phone for any reason. Any exception to this policy must be requested and approved by Treasury & Investments and the SLU PCI Compliance Committee.

D. Special Events Loaner Credit Card Terminals

For special one-time events, the University provides departments with the option to loan a Clover swipe terminal over cellular connection. The wireless terminals may be requested from Treasury & Investments by completing the Special Events Loaner Credit Card Terminal Request Form. Prior to issuance of the terminals, all users must complete the PCI Security Training and agree to the terms of the Special Events Loaner Credit Card Terminal Policy.

E. SLU Marketplace

The SLU Marketplace is a campus wide e-commerce system offered to Saint Louis University departments. The Marketplace provides a departmental solution for creating, managing, and operating online stores including electronic storefronts, shopping cart functionality, secure interfaces for third party applications and Workday integration. The SLU Marketplace tools allow departments to build branded websites, sell tickets, promote events and much more. To request a Marketplace Merchant or Store, please email slumarketplace@slu.edu.

F. E-Commerce & Software

Any department with a need to accept credit cards through the internet via a web application (e-Commerce) must contact Treasury & Investments to coordinate web-based payment solutions with the payment processor under contract with the University.

Server-based software applications and point-of-sale (POS) systems (i.e. cash registers, event ticket distribution) that collect and transmit credit card data for payment must be certified as PCI DSS compliant and listed on VISA's List of Validated Payment Applications. This list can be found on Visa's website at http://usa.visa.com/. Any department interested in implementing a server-based software application or POS system in order to accept credit card payments must notify Treasury & Investments to ensure PCI DSS compliance. PCI DSS compliance certification must be requested annually for all service providers. Proof of certification must be submitted to merchantservices@slu.edu.

G. Third Party Service Providers

Third-party vendors are classified into categories. The first category refers to third-party vendors that contract to do business with and accept credit and debit card payments on behalf of a University merchant. The payments accepted by these third-party vendors must deposit to the University's bank account. These third-party systems are used to meet specific business needs of University merchants.

The second category of third-party vendors refer to vendors who contract to do business at a location on Saint Louis University property. It is imperative the initiating department ensures these third-party contracts with the University address compliance with PCI DSS. All third party service providers must be reviewed and approved by Treasury & Investments and the SLU PCI Compliance Committee. Verification of third-party PCI DSS certification should be submitted to merchantservices@slu.edu annually. This applies to any third-party processing merchant card transactions on behalf of the University, regardless of ownership of merchant.

Departments are not authorized to execute contracts with any third party service provider without prior approval from the Treasury & Investments & the SLU PCI Compliance Committee. See section VI below for policies regarding contracts.

H. Third Party Payment Gateway

A Third-party payment gateway is used to process credit and debit card transactions securely from outside the University environment, relieving the University's liability of maintaining and storing credit card data, provided all other internal security measures are taken. The University has contracted with a third-party payment gateway for the acceptance of credit cards via the internet. This gateway is to be used for all University internet credit card activity.

Any exceptions to this policy and/or contracting with a third party gateway must be approved by Treasury & Investments and the SLU PCI Compliance Committee. Verification of third-party PCI DSS certification will be required upon granting approval. If approved, proof of certification must be submitted to merchantservices@slu.edu, and annually thereafter.

VI. Establishing Contracts

All contracts for payment processing systems or services must have prior approval from the SLU PCI Compliance Committee, Business Services and Office of General Counsel. For e-commerce systems, Information Security and Compliance must also approve security policies and system architecture. This includes agreements for the lease or purchase of software or hardware as well as the outsourcing of any payment system development or management. It is the responsibility of the University merchant to ensure that applicable vendors are PCI compliant at the time of signing as well as throughout the life of the contract.

In some cases, a third party may suggest that payments be processed under that company's merchant ID rather than one owned by the University. Prior approval for these arrangements must also be obtained from Treasury & Investments and the SLU PCI Compliance Committee. Other approvals may be required due to the business nature of the case.

VII. Security and Internal Controls for Merchant Card Processing

Establishing appropriate internal controls and documenting credit and debit card processing and handling procedures ensures the good stewardship and PCI DSS compliance of credit and debit card transaction information. Each department that accepts, captures, stores, transmits, or processes credit or debit card payments through automated systems or manual processes must exercise the following internal controls and follow the required procedures listed below:

A. Card Data Security:

- 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) on mailings or any other physical document.
- Full credit or debit card numbers should never be written down.
- Employees are instructed not to share cardholder information with other employees unless deemed necessary by a supervisor.
- Sending unprotected PANs (primary account numbers) by end user messaging technologies is not permitted.
- Printing the entire PAN (primary account number) on either a department copy or customer copy of any receipt or report is not permitted.
- Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both customer and merchant receipts, and on any reports that may be produced by the device.

B. Protection of Devices Against Tampering

- Any schools/departments with access to credit card processing equipment including point of sale swipe devices or terminals must maintain a record of all devices including, terminal name, model number, serial # and location description of device. The purchase of any device or equipment used to process credit card information must be requested and approved by Treasury and Investments and the PCI Compliance Committee.
- Schools/departments must take protective action against tampering to prevent against the unauthorized capture and use of payment data for fraudulent purposes. Protective action against tampering includes:
  - Periodic inspection of devices.
  - Ensuring only authorized staff have access to credit card processing devices.
- Departments must inspect their point-of-sale devices at a minimum on a quarterly basis for any evidence of tampering and prevention of skimming attacks. All credit card processing terminals/devices must be inspected monthly by each location's Merchant Manager. The Merchant Manager is responsible for completing the Monthly Credit Card Terminal Inspection Form for each terminal/device at each location. Each merchant processing location must maintain records of the Monthly Credit Card Terminal Inspection Forms. Merchant credit card processing locations are subject to periodic site visits by Treasury and/or internal PCI auditors. If suspicious activity or skimming devices are detected on or

around your credit card processing terminal or equipment, please notify merchantservices@slu.edu.

- Any merchant who allows a device or equipment to be used outside the merchant's primary location must maintain a log including the following information:
  - Device model and serial number
  - Employee name and signature
  - Date and time signed out and returned.
  - Event name or reason
  - 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 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 Treasury Services is notified by Fiserv, the University's merchant processor.
- The merchant must respond to the dispute through Fiserv's online portal called Myclientline. The merchant must submit the required documentation of the transaction and retain a copy of the submitted materials along with the sales draft request, including the date the dispute documentation was submitted. There is a limited amount of time for the merchant to respond, so promptness is critical. If the Merchant is not authorized to respond to the dispute, Treasury & Investments will coordinate with Merchant.
- Merchants should periodically review their chargebacks to see if there are internal policies that need to be changed in order to minimize the number of chargebacks.
- Merchants experiencing frequent chargebacks, or who may suspect fraud must contact merchantservices@slu.edu immediately.

G. Storage

- The University does not permit any merchant to store or maintain documents containing the full credit or debit card account number.
- Merchants who justify a business need for requesting credit card or debit card information through mailings or phone must be reviewed and approved by Treasury & Investments and the PCI Compliance Committee. Documents received containing credit or debit card information must be stored in a secure location, processed within one business day, and destroyed immediately.
- Cardholder data storage where credit card number is truncated or blacked out should be stored at a maximum of 2 years.
- Credit and debit card information may NOT be stored on the hard drive of any personal computer, laptop, tablet, or smartphone, on the hard drive of any computer server or network storage device, or any removable storage medium, such as DVDs, CDs, thumb drives, USB keys, etc. Do not store cardholder data in spreadsheet, word processing, database, or other software.
- Cardholder data should not be stored on the POS terminal.
- Merchants may not store or retain in any form the following: the 3-digit Card Validation Value or Code (CID/CAV2/CVC2/CVV2) located on the back of the card within the signature panel, and magnetic stripe data (CAV/CVC/CVV/CSC). In the case of internet transactions, cardholder account numbers must always be encrypted. To confirm internet transactions are encrypted, please contact merchantservices@slu.edu.

- Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, access to cardholder data should be restricted to a "need to know" basis.
- Keys or combinations that allow access to storage of credit card data must be immediately collected or changed in the event a user's responsibilities no longer require him or her to access such documents or systems.

H. Destruction Requirements:

- All credit or debit card information must be destroyed as soon as it is no longer necessary, and may not be retained for more than 90 days after the transaction is processed. In the event of a critical business need, or for legal or regulatory reasons, cardholder data needs to be retained for longer than 90 days, approval must be obtained from Treasury & Investments and the SLU PCI Compliance Committee.
- All Physical documents that are no longer necessary must be cross-cut shredded using a commercially available shredding device approved by the SLU PCI Compliance Committee.

VIII. Merchant Card Transactions-Accounting

Reconciliation and deposits of merchant card transactions must be performed on a daily basis. Ad Hoc Bank Transactions are performed to ensure funds are credited to the respective Workday fund(s). The funds for the merchant card transactions are electronically deposited into the University's bank account and reconciled to the Ad Hoc Bank Transactions by Accounting on a monthly basis. Any discrepancies are communicated monthly to University merchants. If department's do not respond timely to resolve discrepancies, funds will be credited to the University's general fund unless instructed otherwise. All merchants are responsible for complying with this policy, the Saint Louis University Credit Card Deposit Policy and Procedures and for developing and maintaining detailed, written departmental procedures for merchant card processing.

IX. Merchant Card Processing Fees

Merchants are responsible for fees and other costs associated with merchant card processing. The associated startup and recurring costs include, but are not limited to:

- Fees for credit card transactions.
- Hosting services, equipment costs, application and database development and maintenance.
- Resources to implement and maintain merchant equipment.

Merchant processing fees are charged monthly to the University's bank account. Fees are charged to the University bank account around the 3rd business day of the month for previous month's activity. Fees are not journalized until the following month (example: fees charged to the bank account in October for September activity are not charged to the department Workday fund until November). The fees will be charged to the Workday fund indicated on the Merchant Services Account Request/Maintenance Form.

X. Roles and Responsibilities

Merchant

A University merchant is any Saint Louis University business unit that accepts credit and debit cards as a form of legal tender, including retail and web-based operations. University merchants are responsible for compliance by the University's third-party service providers who accept debit/credit payments that deposit to the University's bank account.

Merchant Manager

The Merchant Manager is responsible for compliance with this policy and the related procedures within this manual as well as complying with PCI DSS and University Policies and Procedures. The person assigned as the Merchant Manager must have sufficient level of management authority within the department and will be responsible for ensuring all individuals who handle and process credit and debit card transactions have completed the PCI Security Training prior to handling credit and debit card data. The Merchant Manager is also responsible for documenting and maintaining departmental merchant card policies and procedures.

Merchant Processing Users

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 Credit Card Processing procedures and any associated documents to protect cardholder data. Users must complete PCI Security Training annually and upon hire.

PCI Compliance Committee

The SLU PCI Compliance Committee was established by the University and is led jointly by Information & Technology Services and Treasury & Investments and includes members from various areas of the University who are involved with merchant card handling and processing. The committee serves in guiding and monitoring the University's CDE to ensure compliance with PCI DSS.

IT Staff/Information Security & Compliance

The Office of Information Security & Compliance has a governance role to oversee that appropriate IT Staff properly address the configuration and management of all computer systems and other IT resources in order to meet compliance with PCI DSS and Saint Louis University security requirements, and thus limit access to IT resources that process, transmit and store cardholder data.

Treasury & Investments

Treasury & Investments is responsible for the oversight of merchant card processing including the initial setup and ongoing administration of all Saint Louis University merchant accounts. Treasury & Investments is responsible for establishing and maintaining University policies and procedures and managing user PCI training.

Contact Information:

For questions or comments regarding this policy, PCI Compliance and/or merchant card handling or processing, contact:

Email: merchantservices@slu.edu
Phone: (314) 977-7073

For additional merchant processing information, please visit the Treasury & Investments website.

APPENDIX A – Inspecting the Terminals

In addition to the periodic University Terminal Inspection Form, further procedure checks should be completed.

Procedure checks could include:

- Checking serial numbers & terminal identifiers against the inventory
- Checking the small screws on the base of a terminal are tight and secure.
- Checking tamperproof serialized security tape is in-place and undamaged.
- Checking the edges of a terminal have not been pried apart to insert a device inside.
- Checking that there are no unusually large gaps, scuffs or scratch marks that might suggest the terminal has been opened by force.
- Checking that no cables have been changed or extra cables added to the terminal.
- Taking photographs of the terminal and referencing current photos against known good images
- Weighing the terminals; if someone has attached an additional device or card skimmer onto the device it will change the weight of the terminal.

This isn't an exhaustive list of checks that could be performed, nor will it be appropriate to perform all listed checks for all terminals in all possible locations. It is an example of the types of activities that should be considered when developing a terminal inspection procedure.