PCI-DSS Compliance Policy

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Prepared By</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version # 1.0</td>
<td>Quality Assurance Office</td>
<td>314-977-1654</td>
</tr>
</tbody>
</table>

**Divisions or Departments Affected:** Information Technology Services

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>Last Updated:</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/29/10</td>
<td>New Policy</td>
</tr>
</tbody>
</table>

**Approved By:** T. Brooks, V.P., CIO

**Approval Date:** 09/29/10

**Audience**
This document applies to all Saint Louis University information resources, organizational units and workforce members that transmit, receive, initiate and/or receive electronic financial transaction data through the use of a credit or debit card and its respective application and database Business Owners and Users located on the SLU PCI Certified Network.

**Responsibilities**

*Executive Sponsor*  
SLU Information Technology Services Chief Information Officer

*Key Stakeholders*  
Saint Louis University, Saint Louis University Information Technology Services Information Security, Organizational Unit Business Owners that execute credit/debit card transactions.

*Document Owner*  
Saint Louis University Quality Assurance Office

*Document Management*  
The document owner is responsible for the publication, notification and maintenance of this document. The Executive Sponsor is responsible for approving all changes to this policy.

*Implementers*  
All Saint Louis University Organizational Units that conduct financial transactions on behalf of the University and its respective personnel and departments responsible for ensuring that the requirements in this document are implemented.
Table of Contents

APPROVALS ................................................................................................................................. 3
INTRODUCTION ............................................................................................................................ 4
PURPOSE ..................................................................................................................................... 4
SCOPE ......................................................................................................................................... 4
RISK OF NON-COMPLIANCE ..................................................................................................... 4
DEFINITIONS ............................................................................................................................... 4
POLICY ....................................................................................................................................... 5
  METHODS OF PROCESSING ...................................................................................................... 6
  CRYPTOGRAPHIC/ENCRYPTION KEY MANAGEMENT ............................................................ 6
ROLES AND RESPONSIBILITIES ............................................................................................... 7
APPROVAL AND AMENDMENTS ............................................................................................... 7
POLICIES OR PROCEDURES REFERENCED .............................................................................. 7
QUESTIONS ABOUT THIS POLICY ........................................................................................... 8
ADDENDUM(S) ............................................................................................................................. 8
ADDENDUM A ............................................................................................................................. 9
## REVISION CHART

<table>
<thead>
<tr>
<th>Version</th>
<th>Primary Author(s)</th>
<th>Description of Revision</th>
<th>Date Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>D. Davis</td>
<td>Initial Version</td>
<td>9/24/10</td>
</tr>
</tbody>
</table>

## APPROVALS

<table>
<thead>
<tr>
<th>Version</th>
<th>Approver(s)</th>
<th>Organizational Unit</th>
<th>Date of Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>D. Davis</td>
<td>Quality Assurance Office</td>
<td>9/28/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Security Compliance</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>K. Aubuchon</td>
<td>Quality Assurance Office</td>
<td>9/28/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Security</td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>A. Waheed</td>
<td>Director ITS Administration</td>
<td>9/28/10</td>
</tr>
<tr>
<td>1.0</td>
<td>T. Brooks</td>
<td>Vice President, Chief Information Officer</td>
<td>9/28/10</td>
</tr>
</tbody>
</table>
INTRODUCTION
The Payment Card Industry (PCI), including VISA, Master Card, AMEX, Discover and other major card issuers, has established important and stringent security requirements to protect credit card data. These are called the PCI Data Security Standards or “PCI-DSS.” This policy defines the way in which credit card merchant accounts must protect cardholder data and achieve PCI-DSS compliance based on the method that credit cards are processed.

PURPOSE
The purpose of this policy is to clearly define the roles and responsibilities for all stakeholders classified as Merchant Account Holders (MAH) and the requirements to comply with the PCI-DSS in association with the transmission, storage and processing of credit/debit card data.

This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council at: https://www.pcisecuritystandards.org/.

SCOPE
This policy applies to each organizational unit which processes credit and debit cards.

RISK OF NON-COMPLIANCE
Without adherence to the PCI-DSS standards, the university would be in a position of unnecessary reputational risk and financial liability. MAH’s who fail to comply are subject to:
  a. Any fines imposed by the payment card industry;
  b. Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees;
  c. Suspension of the merchant account;
  d. Reputational loss; and
  e. Potential for civil and/or criminal litigation.

DEFINITIONS
- **PCI-DSS** – Payment Card Industry Data Security Standard this is industry security standard that is utilized to audit and insure compliance for credit/debit card transaction processing.
- **PA-DSS** – Payment Application Data Security Standard this is the certification process that applications that process credit/debit transactions must go through for an organization to process payments. Effective July 2010, every organization must insure that they are using PA-DSS certified applications and hardware or face potential monetary fines and penalties.
- **ITS Quality Assurance Office** – A group within Information Technology Services that assists in managing the information security, compliance, logical access, change management and other policies and processes that insure protection of the University’s information resources.

Compliance is responsible for insuring that the effected organizational unit/department within the university is compliant and auditable with/by PCI-DSS and PA-DSS standard requirements. This function works with the effected organizations/departments to achieve and maintain compliance to pass audits successfully.

Additionally, this Office will assist/advise on policy, procedures, processes, controls, pre-audit preparation, controls testing, risk assessments, internal/external audit activities, and function in an advisory capacity with new applications, hardware, procedures, processes and any other activities that involve information and data security inclusive of PCI but not excluding the requirements of federal, state, regulations and university policies, procedures and processes.
• **ITS Operations** – A group within Information Technology Services that assists in managing IT infrastructure support and operations.

• **Information Technology Services (ITS)** – responsible for network, infrastructure hardware, software, devices, communications, application and database data security, federal, state, university information security adherence, third party vendor security and approvals, audit and compliance to/for University information technology assets.

• **Business Owner** – purchaser/responsible party and user of the application and/or database being used for their business purposes along with Payment Processing Hardware and/or third party vendor(s).

• **System Administrator (SA)** – person(s) assigned to managed and administer all information technology activity and user accesses for a Business Owner’s application and database. The SA is the only individual with Administrator rights to servers, databases and local workstation.

• **Merchant Account Holder (MAH)** - the organizational unit that has the electronic payment processing account.

• **Information Resources** - Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Information Resources includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

• **Organizational Unit** – An entity within the University that operates as a distinct function, such as a department, division, business unit, school, college and/or library.

• **User** – Any person accessing University information resources.

• **Workforce** - Employees, volunteers, trainees, contractors, and other persons under the direct control of the covered entity, whether or not paid by the University.

**POLICY**

1. Business Owners of the applications and databases will support their assigned System Administrators for application and database support and administration.
   a. Only the System Administrator will have Administrator Access to the Server, Workstations, Application and Database.
   b. The Business Owner will follow the established process for Logical Access request in granting User Rights to their respective application and data base based upon the person(s) job description and role.
   c. This excludes any request for administration rights of any type on any system, hardware, application, database, network or storage device.
   d. No local machine Administrative Rights will be allowed to be assigned to or by the Business Owner.
   e. Requests for any application or database related updates or system upgrades or maintenance by a Business Owner will be managed by the ITS Operations System Administrator assigned to the Application and Database.
      i. The Business Owner is expected to collaborate with and aid in planning the activity that needs to be performed to their respective system(s).
2. Local and Server Administration Rights will be granted on an as needed basis to the Business Owner and only for a short/temporary period of time as is required by the activity that is needed to conduct/execute an action.
   a. A Change Control Ticket will need to be initiated and the change control process followed.
b. This activity will be monitored and logged by the System Administration Operations Group.

3. The Business Owner, their staff, contractors, temporaries and interns will on an annual basis, participate in and provide the requested documentation for a PCI Self-Assessment conducted by ITS in addition to the Annual Audit performed by an External Auditor.

4. The Business Owner will work collaboratively with ITS to draft, review and update on an annual basis, their organizational policy and procedures as they relate to the PCI-DSS standards and apply them to their daily business processes for the applications, databases and any third party vendors.

5. The Business Owner is to review and validate on an annual basis that their payment processing hardware remains in a compliant status with PCI-DSS. If it is discovered that the equipment has become non-compliant, the Business Owner will notify the Quality Assurance Office. The Business Owner will coordinate with the appropriate parties and Quality Assurance and will replace the non-compliant equipment within 30 days.

6. Any other circumstances that may occur will be managed through the exception process, which will be reviewed by ITS, and senior and or executive management on a quarterly basis for continuation of allowance of the exception. Or, an amendment/update to this Policy can be proposed.

7. When there is new payment transaction software needed or an upgrade to an existing product these must be authorized by the appropriate management levels, inclusive of Information Technology and Information Security reviews and approvals. The software will be downloaded by the IT department and the designated SA, following the Change Control Processes.

METHODS OF PROCESSING

1. Only the following methods for processing are allowable.
   a. Point of Sale (POS) processing using dedicated phone lines for both card present and card not present (received by mail, phone or fax) transactions.
   b. Web-based processing using a PCI-compliant service provider approved by Information Security and the Treasurer’s Office such that the credit card number is NOT entered into a web page of a server hosted on PCI VLAN SLUNet.
   c. PCI-compliant third party hosted processing in which credit card data is not stored or transmitted on the PCI VLAN SLUNet.
   d. Applications and Hardware in use must be PCI-DSS, PA-DSS certified.

2. All new and existing processors must be approved by Information Security and the Treasurer’s Office on an annual basis.

CRYPTOGRAPHIC/ENCRYPTION KEY MANAGEMENT

Cryptographic keys will be managed by the ITS Operations Group System Administrator of the respective applications and databases and/or devices. They will not be managed or administered by the Business Owner.

1. The ITS Operations Group System Administrator of the respective applications and databases and/or devices is responsible for initiating the procedure for the key change process at its respective cycle. The Quality Assurance Office is responsible for the overall oversight of the procedure.

2. Cryptographic keys will not be managed or administered by the Business Owner.

3. Key Management Exception
   a. The ONLY type of cryptographic key management exception that Saint Louis University Information Security authorizes and manages to is the type in which an application that has an automated system generated menu selection which initiates the application process to...
generate a new key on the prescribed schedule. This is an exception to the SLU “Controls For Credit Card Transactions” Policy.

b. With the only exception being “a” above, per SLU Policy, there is not to be human intervention, generation of, knowledge of, handling or storage of any cryptographic keys whatsoever.

c. If situations occur in which there is an exception needed to “a” or “b”, the exception will be presented to ITS Information Security for a case by case exception review and ruling.

4. Cryptographic Key(s) will be generated at a minimum on an annual basis per PCI-DSS requirements. Each application and database will be assessed on an individual basis and a determination made by Information Security and Compliance if a more frequent schedule needs to be created.

5. Data encryption management and/or application specific procedures are located in the attached addendum(s).

6. Use of alternative methods may be requested, reviewed and approved, on a case-by-case exception basis jointly by Information Security and the Treasurer’s Office. Information Security will provide the final approval.

ROLES AND RESPONSIBILITIES
It is the responsibility of SLU workforce members to read, understand, and follow this policy. Any person with questions regarding the application or meaning of these guidelines should seek clarification from his or her supervisor or the document owner.

RESPONSIBILITIES

1. The Quality Assurance Office, including information security compliance staff, is responsible for oversight, compliance and participation in all audit and compliance activities relating to PCI-DSS compliance by all application, database, network and overall systems and infrastructure compliance to the PCI regulations.
   a. This is inclusive of all applications utilized for credit/debit card transaction activities whether it is on the SLUNet, third party application, or a hosted solution across all organizational units at Saint Louis University.
   b. The Quality Assurance Office Information Technology Staff are additionally responsible for participation, oversight in any technology audit being conducted whether by internal or external parties.

2. ITS Operations are responsible for the management and administration of applications, associated databases, infrastructure and hardware to manage the PCI environments.

3. The Business Owner will not have any administrative rights to either the application or database and will follow documented User Access Requests and Change Control to grant user access and rights for daily use of the product(s).

APPROVAL AND AMENDMENTS
Changes to this policy may be necessary from time to time. At a minimum, this policy will be reviewed and approved annually. All changes to this policy will be approved by the Executive Sponsor. Documentation, including a record of all changes to the charter, will be maintained the Document Owner and will be stored on the ITS internal Google site.

POLICIES OR PROCEDURES REFERENCED

ITS Information Security Policies
QUESTIONS ABOUT THIS POLICY

If you have questions about this Policy, please contact the Quality Assurance Office at qaoffice@slu.edu. Failure to follow this procedure can result in disciplinary action as provided in the Staff Employee Handbook, any Student Worker/Intern employment information and Faculty Handbook. Disciplinary action for not following this procedure may include termination, as provided in the applicable handbook or employment guide.

ADDENDUM(S)

Where appropriate and as noted in an addendum, PCI applications will be listed. Separate Standard Operating Procedures documentation will be developed for each application and its affiliated systems and published to the ITS website in a protected format.
ADDENDUM A

PCI Application Listing

1. Visual 1 Property Management System – Water Tower Inn