Payment Card Processing Policy at UST

Purpose
In order to create a secure environment for acceptance and processing of payment ("credit/debit") card information at the University of St. Thomas ("University" or "UST"), the following guidelines have been established in accordance with the Payment Card Industry Data Security Standards ("PCI DSS").

Scope
This policy pertains to all University of St. Thomas departments at all campuses and affiliated locations that accept, process, transmit, and/or handle payment card data on behalf of the University. Every employee, regardless of status as student, contract, regular, FTE, or other, is responsible for adhering to these guidelines. All departments handling payment card data must also comply with the PCI DSS.

Merchant Identification Numbers
A merchant identification number ("MID") is required for processing payment card transactions. The MID is issued by UST’s Acquiring Financial Institution and all individual numbers will fall under the greater UST umbrella.

Due to the expense and liability of accepting card payments, a determination must be made as to whether the benefits of card acceptance exceed the liabilities. If it is determined that the requesting department should have the ability to accept card payments then the department will work with staff from the Business Office and Information Resources and Technologies ("IRT") to determine the appropriate method of acceptance.

Third Party Processors
All merchant departments at the University must use the approved third party vendor for processing payment card transactions. Should the functionality provided by the approved vendor not meet the needs of the department, a request must be made and approval obtained to use a different third party vendor. Request should be submitted to UST's PCI Committee.

All third party vendors must be PCI DSS and Payment Application Data Security Standard ("PA DSS") compliant and acknowledge their security responsibility as a contractual requirement. The third party vendor should:
  - be listed on Visa’s Global List of PCI DSS Validated Service Providers
  - and/or furnish the University a copy of their PCI DSS compliance letter.
  - also be able to provide the University with a summary of their business continuity or incident response plan in the event of a security breach or other emergency.
Payment Card Acceptance Methods

There are several ways in which payment card data can be collected for payment processing; internet, phone, fax, mail, and in person. **Under no circumstances should email ever be used to relay payment card information!**

It is highly recommended that, whenever possible, payment card transactions be handled completely electronically through an approved secure payment application processor. For security purposes it is always best when the cardholder is able to enter their own information directly into the payment application. However, it is recognized that an online option is not always available. Therefore, the following guidelines must be adhered to when handling physical payment card data:

- Physical payment card data must be locked in a secure area when it is not of immediate use for processing
- Access to physical payment card data should be restricted on a 'need to know' basis
- Only essential information should be stored
- **Never** store the three-digit card validation code printed on the signature panel of a payment card (referred to as CAV2, CID, CVC2, or CVV2)
- Sensitive payment card data should **never** be kept electronically in a spreadsheet, text document, or other similar electronic file
- Sensitive payment card data should **never** be downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers, or personal digital assistants
- Payment card data should be retained only for the time necessary to process. UST approved third party vendor provides a transaction ID number in the event that a transaction needs to be revisited
- When payment card data is no longer needed, it should immediately be destroyed using a cross-cut shredder
- All payment card receipts must display truncated payment card numbers only
- Faxes containing payment card data should be limited to fax machines with access restricted to only those individuals responsible for processing the card transactions and not connected to the UST email system.
- Appropriate segregation of duties shall be maintained between payment card processing, the processing of refunds, and the reconciliation function. A secondary approval for all refunds must be obtained.
- Wireless networks will not be used for any payment card administration unless it has been approved by the IRT security team.

Employees Responsible for Payment Card Processing

For employees who will participate in any part of the payment card acceptance process, the following shall apply:

- Potential employees will be screened during the hiring process by completing a background check
- Employee must visit the Business Office PCI DSS webpage at least once every 12 months to review policies, procedures, updates, and best practices. Contact the Business Office for additional training opportunities.
Employee will provide written acknowledgement that he/she has read and understood the University’s Payment Card Processing Policy and his/her responsibilities regarding payment card acceptance and PCI DSS accordingly.

Technical Information

All payment card payment systems used at UST will comply with PCI’s Payment Application Data Security Standard (“PA-DSS”). All transactions that involve the transfer of payment card information must be processed on systems approved by UST PCI Committee and signed off on by the University’s CFO.

The system will be examined using the PCI Self Assessment Questionnaire (“SAQ”) to determine if the system complies with the PCI requirements. When all requirements of the SAQ are met and the system is deemed to be compliant, a report will be sent to the CFO detailing the compliance so that they can sign off on the system. If there are significant costs or effort required to bring a new payment card system into PCI compliance, or the new system would require a change in UST’s PCI level or status, approval of the CFO and CIO will be required.

The Requirements:

1. Install and maintain a firewall configuration to protect data.
   a. Systems should reside within our firewalled data center if possible.
   b. Systems not in the data center should be isolated and firewalled from other networks.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
   a. All passwords should be changed before the system goes live.
3. Protect stored cardholder data.
   a. Cardholder data is protected and only necessary elements stored.
4. Encrypt transmission of cardholder data across open, public networks.
   a. Minimize any transmission of data and ensure any transmission is encrypted.
5. Use and regularly update anti-virus software.
   a. Any computer used will run anti-virus software and be maintained and updated regularly.
6. Develop and maintain secure systems and applications.
   a. Vendor-supplied software will be maintained and updated when new versions and patches become available.
7. Restrict access to cardholder data by business “need to know”.
   a. Access to the system is “need to know” only.
8. Assign a unique ID to each person with computer access.
   a. System access is controlled by unique ID.
b. Vendor access to PCI related systems is enabled only when needed.

9. Restrict physical access to cardholder data.
   a. Data in any form (electronic or paper) is physically secured from unauthorized access.
   b. Any paper data is destroyed when it is no longer needed.
   c. Employees who use credit card terminals will periodically inspect the device surfaces to detect tampering.

10. Track and monitor all access to network resources and cardholder data.
    a. Not applicable to SAQ C. Only required for PCI systems that store payment card data.
    b. UST is not funded to implement systems that store payment card data.

11. Regularly test security systems and processes.
    a. External scans performed by approved vendor.
    b. Any suspected security incidents on the PCI network will be followed up with a thorough investigation following the procedures in the UST Incident Response policy.

12. Maintain a policy that addresses information security.

Administration and Enforcement
The University of St. Thomas Business Office, in conjunction with IRT, is responsible for oversight and management of the Payment Card Processing Program at the University. Issues, questions, concerns, or requests should be directed to the Associate Director of the Business Office. IRT should be contacted immediately if a breach in data security is suspected at IRTTechdesk@stthomas.edu or 651.962.6230.

The Business Office and IRT reserve the right to perform both annual audits and unannounced audits of campus merchants. Full compliance with these requests is expected.

Failure to follow the guidelines established within this document will result, at a minimum, in the suspension of privileges to accept payment cards. Major violations of this policy by campus merchants could result in (but not limited to) fines by the card providers, restitution for any resulting damages, and damage to the reputation of the University of St. Thomas.