Purpose

The University has adopted the following policy and supporting procedures for all types of credit card activity transacted in-person, over the phone, via fax, mail or the Internet. The purpose of this policy is to protect the interests of the University and its customers by establishing strong internal business controls and standard revenue collection methods throughout the University.

This policy provides guidance so that the processes of accepting electronic payments comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the University's financial and other systems. In addition, adherence to this policy will ensure compliance with Sections 35.61, 72.004 and 502.002 of the Texas Business & Commercial Code, related to the protection of credit/debit card information and other personal identifying information.

UT Dallas has contracted with a third-party vendor whose core business includes the support and processing of credit card and electronic transactions. The vendor provides the University with a secure gateway and hosted solution in which all electronic personal payment information is securely transmitted to and stored on off-site computers which the company owns and maintains. The vendor maintains PCI DSS compliance certification. This relationship enables the University to provide secure infrastructure for acceptance of electronic payments.

Applicability

Any UT Dallas employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card and electronic payments is subject to this policy. Failure to comply with the terms of this policy may predispose the department and/or the University to financial losses and/or legal liabilities.

Policy Statement

Any department electronically collecting revenue (through credit cards or electronic checks) on behalf of the University for goods or services must utilize a secure web based storefront. "Marketplace" is the University's preferred web based application for electronic collection of revenue. This application can accommodate receipt of checks and credit cards (Master Card, Visa, American Express, and Discover) in a secure environment which is maintained by the third-party provider as referenced in the Purpose section. If a department believes that it has a significant business case or processing requirement that cannot be achieved using Marketplace it may be granted authorization to use other credit card processing systems (see Exceptions to Using Marketplace).

Responsibilities of a Merchant Department

The following responsibilities are an important aspect of the University's compliance with the PCI Data Standards. Any department collecting revenue on behalf of the University is considered a Merchant Department. The Merchant Department must designate an individual who will have primary authority and responsibility for revenue collection within that department. This individual will be the designated Merchant Department Representative or "MDR".

Credit Card Acceptance Policy

SUB-TOPIC
Policy for Accepting Credit Card and Electronic Payments

All Merchant Departments must:

1. Complete the Application to Become a Merchant Department (see Attachment A).

2. Follow the Card Acceptance guide (or similar rules) of the merchant processor/acquirer (e.g., Global Payments) and the operating regulations and rules of any card associations/networks that will be accepted by the Merchant Department (e.g., MasterCard, Visa, etc.). Links to Global Payments, MasterCard and Visa are provided for reference:

    - Global Payments Card Acceptance http://www.globalpaymentsinc.com/myglobal/cag.html
    - MasterCard Worldwide Rules and Chargeback http://www.mastercard.com/us/merchant/support/rules.html
    - Visa Merchant Responsibility and Card Acceptance Guide http://usa.visa.com/merchants/new_acceptance/merchant_responsibility.html

3. Ensure that all employees, including the MDR, contractors and agents with access to payment card data complete compliance training on an annual basis.

4. Revenue collection arrangements that require payees to enter credit card numbers on preprinted order forms which are then mailed to a UTD department are not allowed.

5. Ensure that all credit card data collected, regardless of how it is stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Numbers) is secured. Data is considered to be secured only if the following criteria are met:

    - Only those with a need-to-know are granted access to credit card and electronic payment data.
    - Email is not used to transmit credit card payment information. If the use of email is necessary, only the last four digits of the credit card number are displayed.
    - Credit card or electronic payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
    - Fax transmissions (both sending and receiving) of credit card and electronic payment information are limited to those fax machines whose access is restricted to authorized individuals. The transactions must be processed immediately and the documents must be shredded.

- The processing and storage of personally identifiable credit card or electronic payment information on University computers and servers is prohibited. Exceptions can only be made if the processing and storage methods are compliant with this policy, the UT System Information Security Policy and PCI Data Security Standards. These standards detail strict encryption protocols.

- Only secure communication protocols and/or encrypted connections are used during the processing of electronic transactions. (NOTE: The UT Dallas Information Security Department maintains a staff of security professionals who are available, as required, to provide consultative services on appropriate security practices. The Director of Information Security can be contacted for more information regarding these services.

- The three-digit card-validation code printed on the signature panel of a credit card is never stored in any form.

- All but the last four digits of any credit card account number are masked if credit card data is displayed.

- All credit card and electronic payment data that is no longer deemed necessary or appropriate to store is destroyed or rendered unreadable.

- Before accepting check payments, the storefront must contain a disclosure that all checks will be converted into ACH transactions and will be processed electronically. In addition, the receipt should provide written notification of this disclosure.

- All computers accessing or providing support for the web based storefront must be encrypted with McAfee SafeBoot. In addition, Identityfinder must be installed and configured to run weekly. All discovered instances of the full credit card number, bank account number, or social security number must be reported to the Department Head, Treasury Manager, and the Information Security Office and remedied immediately.

6. No credit card receipt or other document referencing the transaction shall include more than the last four digits of the account number or the month and year of the expiration date.

No University employee, contractor or agent who obtains access to credit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to any third party other than to the University's acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request. All requests to provide information to any outside party must be reviewed and approved in advance by the Vice President for Communications and the Vice President for Business Affairs or their delegates.

Process to become a Merchant Department

The MDR or his/her designee must follow the steps below in order to request approval to become a Merchant Department.

1. Notify the Treasury Manager in The Office of Finance of a need to accept credit card and/or electronic payments by completing an Application to Become a Merchant Department.

2. Obtain approval from the school/division Department Head. It is the responsibility of the Department Head to approve the business case and all other information provided in the application, and to approve the designation of the Merchant Department Representative.

3. Submit the signed application to the Treasury Manager for review and approval by the Associate Vice President for Finance and Controller.

4. If the application is approved, the Treasury Manager will forward a request to University Web Services to design a new Marketplace storefront for the Merchant Department. The Merchant Department should allow sufficient time for this process to be completed.

5. The Merchant Department Representative must contact the Information Security Office to schedule installation of McAfee SafeBoot and Identityfinder on the computers that will access or support the web based storefront.

6. The Treasury Manager will arrange the necessary training for the Merchant Department, as well as any additional information pertinent to the approved payment method.

Exception to Using Marketplace

If a department believes that it has a significant business case or processing requirement that cannot be achieved using Marketplace, they must provide the details of their case, in writing. Examples would be departments that have a high volume of walk-in customers that are paying in person, such as The Pub or Bookstore. In this case, the department may be granted authorization to use an alternate credit card processing system or vendor.

If the Merchant Department needs to utilize this alternative, they must:

- Complete the Application to become a Merchant Department. The application should request a release from the Marketplace requirements specified by this policy. The request should include the details of their business case and specific processing requirements.
- Provide proof that the alternate vendor is certified PCI compliant and ensure that the department and its vendor comply with all relevant provisions of the UT System Information Use and Security Policy and the UT Dallas Policy for Accepting Credit Card and electronic Payments (See link at the end of this policy).
- Comply with the requirements for installation and running of McAfee SafeBoot and Identityfinder as described above.

The Treasury Manager will review the department's request, and forward it to the Associate Vice President for Finance and Controller for approval. In the event that the use of an alternate vendor is approved, the Merchant Department will be subject to periodic inspections by the Treasury Manager to ensure compliance with the University policy and the PCI Data Security Standards.

An additional exception to using Marketplace applies to departments accepting donations. All donations to the University should be coordinated by the Office of Development and should use the customized online donation option configured through that office. For assistance in establishing a donation link, users should contact the Office of Development.

Process for Responding to a Security Breach

Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept credit card and electronic payments.

In the event of a breach or suspected breach of security, the Merchant Department must immediately perform the following steps:

1. Contact the Treasury Manager and the Chief Information Security Officer. The Chief Information Security Officer will provide further instructions which will include measures that will preserve electronic evidence.

2. The Chief Information Security Officer will implement a Crisis Response Plan to isolate, investigate, document and remediate the situation in partnership with the Treasury Manager.

3. All investigation and collection of evidence will be done by an Information Security Analyst. To prevent alteration of the compromised system or systems, Information Security asks the MDR to follow the requests below:

    - Do not switch off the compromised machine.
    - Do not attempt to isolate the compromised system(s) from the network by unplugging the network connection cable.
    - Do not log on to the machine and/or change passwords
    - Be on HIGH alert and monitor all electronic applications and report suspicious activity to Information Security.

4. The Treasury Manager shall alert the merchant bank, the payment card associations and the UT Dallas Police Department. The Associate Vice President for Finance shall report the suspected breach to the Vice President for Business Affairs who will in turn take the appropriate actions to alert the President, the Chief Information Officer, the Vice President for Communications, and other relevant regulatory agencies.

5. Where an actual breach of credit card data is confirmed, the Treasury Manager, with the assistance of the Chief Information Security Officer, will ensure that compromised credit card account information is securely sent to the appropriate credit card associations and credit reporting agencies.

6. Within 48 hours of the breach, the Treasury Manager, with assistance from the relevant MDR, shall provide the affected credit card associations with proof of PCI compliance.

7. Within 4 business days of the breach, the Treasury Manager, with assistance from the relevant MDR, shall provide the affected credit card associations with an incident report.

8. At the relevant credit card associations' request and depending on the level of risk and data elements compromised, the University may, within 4 business days of the event:
   - Arrange for a network and system vulnerability scan.
   - Complete a compliance questionnaire and submit it to relevant card association(s).

9. In the event that personal data is exposed, per UT System Information Use and Security Policy #UTS165, the University will provide notification to any resident of Texas and data owners whose personal identifying information was or is reasonably believed to have been acquired without authorization.

Ongoing Policy Management

- University of Texas at Dallas may modify this policy from time to time as required, provided that all modifications are consistent with Payment Card Industry Data Security Standards then in effect.

- The Treasury Manager of the Office of Finance is responsible for initiating and overseeing an annual review of this Policy, making revisions and updates and ensuring that the updated policy has received the appropriate approvals and is distributed to the Merchant Departments.

Attachments

Attachment A - Application to Become a Merchant Department
Attachment B - PCI Data Security Standards
Attachment C - UT System Information Use and Security Policy – UTS165

Legal Statutes

Texas Business & Commercial Code, Section 35.61
Texas Business & Commercial Code, Subchapter A, Chapter 72
Texas Business & Commercial Code, 502.002