Texas A&M University-San Antonio

21.01.02.O0.01 Credit Card Collections
Approved: October 14, 2013
Revised: November, 2015
Next Scheduled Review: November, 2020

Procedure Statement

Texas A&M University-San Antonio (A&M-San Antonio) offers university departments the convenience of accepting credit cards as payment for goods and services provided. With prior approval, departments may accept credit card payments over the counter, over the phone, or over the internet. Supplemental information regarding the program can be found at http://www.tamusa.tamus.edu/ SBS/PaymentOptions.html.

Reason for Procedure

The purpose of this Procedure is to ensure documented procedures, proper training, and proper physical storage and access to credit card data are followed.

Official Procedure

1. ESTABLISHING NEW MERCHANT ACCOUNTS

1.1 Merchant Accounts must be in place before credit cards may be accepted. Accounts can be revoked for failure to comply with credit card processor guidelines or University Rules or Procedures. Departments that decide to accept credit cards must make a direct request to Financial Services. Departments should contact Financial Services to determine the best solution to their credit card collection needs. Financial Services will establish a new merchant account through the credit card processor on the department's behalf. New merchant account activation typically takes 3 weeks from the time Financial Services receives the request.

1.2 For departments that plan to accept cards in person, financial services will assist with acquiring the equipment for installation to ensure compatibility with current systems. In certain circumstances, it may be necessary for the department to purchase the equipment. For limited use, the department may arrange to rent equipment. Depending on placement, this equipment requires work orders for telecommunications or AC power accommodations.

1.3 A PCI Compliance Questionnaire must be completed and submitted to Financial Services for each credit merchant setup.

2. CREDIT CARD SALES

2.1 Credit card sales should be recorded like any other sale. Customers should be given receipts verifying payment for purchases unless an exception is granted by the Comptroller.

2.2 To process sales for walk-in customers presenting an acceptable credit card, the card should be run through the credit card machine at the time of the sale to validate the account number. The credit card must be kept within the customer's sight. Any exceptions must be approved by Financial Services.

2.3 To process transactions in which the card is not physically present (such as telephone, fax, or mail orders), departments should contact Financial Services to determine the feasibility of establishing an e-commerce site. Departments unable to establish an e-commerce site must request a credit card terminal through Financial Services.

2.4 Processing "card not present" payments through an e-commerce site presents a much more secure avenue, with fewer PCI DSS compliance issues. If it is absolutely necessary for the merchant to process using their credit card terminal, the following must be obtained in order to process the transaction services:

2.4.1 Customer Name

2.4.2 Credit card account number

2.4.3 Expiration date of the credit card

2.4.4 See section 5 for information on the proper security for these types of transactions

3. REFUNDS

3.1 Credit card refunds cannot be issued for more than the original transaction amount and can only be refunded on the card used for the original purchase. However, refunds cannot be processed back to the originating card more than 180 days after the initial transaction. Refunds beyond 180 days from the original purchase should be rare. In those circumstances, the merchant should first verify that the refund has not already been processed. If the refund has not already been processed, the merchant should submit a payment request to Financial Services Accounts Payable so that a check can be issued.

4. DAILY CLOSE OUT AND DEPOSIT PROCEDURES

4.1 Deposits should be made on a daily basis by someone other than the individual who accepted the transaction payments.

4.2 For credit card sales, the credit card detail report and bill slips should be sent to Financial Services, on a daily basis. This report should break down the Visa/MasterCard, Discover, and American Express totals. If the department has a credit card device with a printer, attach the tape to the credit card detail report.

4.3 Departments are responsible for reconciling credit card deposits to their FAMIS account.

5. CREDIT CARD SECURITY

5.1 A&M-San Antonio and the payment card industry take the safeguarding of data very seriously. Failure to comply with university and industry security regulations may result in the revocation of the department's merchant account or, in the case of lost or stolen cardholder data, assessment of severe fines on the university and department by the bank. **Departments are financially responsible for fines resulting from security breaches that originate from their systems.**

5.2 Before a department can begin to receive credit card payments, they must implement adequate security and internal controls that meet Payment Card Industry data Security Standards (PCI DSS) requirements. To ensure adequate security, the department must request setup and approval from both the Information Technology Services (ITS) and Financial Services departments.

5.3 The design and architecture of computer systems and networks associated with credit card processing, as well as the protocols used to transmit such data, must be approved by the university Information Security Officer (ISO) prior to implementation. Subsequent changes must be approved prior to implementation.

5.4 All equipment and software must comply with current PCI security standards. Non-compliant equipment or software must either be reconfigured or replaced.

5.5 Computer or computer network security and internal controls should include, but not limited to:

5.5.1 Install and maintain a firewall configuration to protect cardholder data.

5.5.2 Protect stored cardholder data through encryption and store as little cardholder data as necessary.

5.5.3 Encrypt transmissions of cardholder data, and never accept credit card data over e-mail.

5.5.4 Use and regularly update antivirus software or programs.

5.5.5 Develop and maintain secure systems and applications.

5.5.6 Restrict computer and physical access to cardholder data to authorized personnel. Prior to storing credit card information on a computer or file server, the department must submit a security plan for approval from both the ISO and Financial Services department. If credit card information is stored on a computer make sure the file is password protected and the credit card information is encrypted. The credit card information should be located on a drive or server with very limited access.

5.5.7 Assign a unique user ID to each person with computer access.

5.5.8 Track and monitor all access to network resources and cardholder data.

5.5.9 Regularly test security systems and processes, in accordance with the most current best practices and PCI Standards.

5.6 Business process security and internal control features should include, but are not limited to:

5.6.1 Background checks should be obtained for individuals authorized to have access to cardholder data, in accordance with PCI Data Security Standards.

5.6.2 When taking a credit card payment from an individual, always keep the credit card within the customer's sight.

5.6.3 Cards should be accepted for no more than the amount of the purchase.

5.6.4 The amount entered into the credit card machine must agree to the purchase or payment amount.

5.6.5 The credit card expiration date should not be included on the receipt.

5.6.6 Ensure that only the last 4 digits of the credit card number should print on the receipt copy given to the customer. Departments must ensure that machines meet this requirement. Notify Financial Services if your machine is not in compliance.

5.6.7 Third-party vendors with access to sensitive cardholder data must be contractually obligated to comply with PCI security standards.

5.6.8 If cardholder data is stored on paper (such as merchant copies of receipts or daily batch reports), make sure the paper is locked up in a location with access limited to those with legitimate business need. Record retention rules must be followed for the length of time the records are kept.

5.6.9 Only authorized personnel should have access to keys to secured areas containing cardholder data.

5.6.10 No storage of cardholder data on electronic media, including USB drives, discs, hard drives of computers or laptops, etc., is allowed.

5.7 In addition to the initial PCI Compliance Questionnaire completed during setup, each department is required to complete an annual PCI self-assessment questionnaire. Different versions of the questionnaire are available based on the manner(s) in which you accept credit cards. Please contact Financial Services if you are unsure about which questionnaire is right for you.

5.8 The ISO will perform periodic reviews of computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data. Financial Services is available to conduct reviews of business procedures to help departments identify ways to better protect cardholder information.

6. DEPARTMENT RESPONSIBILITIES

6.1 Departments participating in the credit card program are responsible for complying with all rules and procedures issued by Financial Services and all PCI Data Security Standards, including periodic business review and completion of the annual PCI questionnaire(s). Departments will provide reasonable assistance necessary to the ISO in the performance of periodic reviews of credit card related computer to computer network security. This includes providing IP addresses and network configuration diagrams for use in scanning systems for vulnerabilities. Departments are responsible for notifying the ISO and Financial Services in the event of a suspected security breach. Departments are required to work with Financial Services to create written departmental guidelines that cover use of terminals, forms, reconciling transactions, record retention, training and any other information to conduct business. A final copy of the department's guidelines should be provided to Financial Services.

6.2 The department must acquire approval in advance from the ISO and Financial Services to have volunteer employees process transactions.

7. FINANCIAL MANAGEMENT OPERATION RESPONSIBILITIES

7.1 Financial Services is responsible for administering the A&M-San Antonio credit card program and for ensuring that participating departments are kept current on all rules, procedures and security standards. Financial Services will coordinate with the merchant bank on behalf of the department, including any suspected security breach. Financial Services will distribute and coordinate the preparation of the annual PCI questionnaire to each department. Financial Services will work closely with both the department and the

ISO to ensure that all necessary security procedures are in place to ensure protection of sensitive credit card data.

8. INFORMATION TECHNOLOGY SERVICES

8.1 The university will contract with a vendor for vulnerability scans of PCI computer systems and may require configuration changes to eliminate vulnerabilities. Third-party vendor scans are required for PCI compliance. Vulnerabilities must be mitigated as soon as practical.

8.2 ITS will perform vulnerability scans of PCI computer systems and will require configuration changes to eliminate vulnerabilities. (see 29.01.03.O0.17 *Guidelines on Network Scanning*) This is both in preparations for and in addition to vendor scans that are required for PCI Compliance. Vulnerabilities must be mitigated as soon as practical.

8.3 (ITS) standards may be stricter than the PCI requirements to meet campus needs.

8.4 (ITS) is responsible for approving the configuration of the departments' PCI computer systems.

9. REQUIRED TRAINING

9.1 All departments' staff who will be involved in the acceptance of credit card data, including ITS staff who support systems that process credit card data are required to complete an on-line PCI Security training course to handle credit card information. Periodic refresher courses may be required.

9.2 The department is responsible for providing sufficient training to volunteers based on the type of transactions volunteers may process.

10. DISPOSAL OF SURPLUS OR NONFUNCTIONAL EQUIPMENT

10.1 When a department no longer needs a particular device to swipe or read credit cards, that card-reader must be returned to Financial Services for handling or disposal. Notify Financial Services if you have a device to be removed from service. This allows Financial Services to insure that all sensitive information is removed from the device.

Related Statutes, Policies, or Requirements

System Policy 21.01 *Financial Policies, Systems and Procedures*

System Regulation 21.01.02 *Receipt, Custody, and Deposit of Revenues*

A&M-San Antonio Procedure 29.01.03.O.01 *Electronic Information Services Access and Security*

A&M-San Antonio Procedure 29.01.03.O0.16 *Network Scanning and Vulnerability Assessment*

A&M-San Antonio Procedure 29.01.03.O0.17 *Incident Management*

Appendix

Payment Card Industry Data Security Standards (PCI DSS)

Texas A&M University Credit Card Merchant Resources

Definitions

Merchant Accounts are special bank accounts issued by a merchant processing bank (also called a credit card processor) that allow a business to accept credit, debit, gift, and other payment cards. University departments or offices with such accounts are hereafter referred to as "Merchants".

Merchant Level: This classification is based on transaction volume. Merchants are ranked as level 1 through 4, Level 1 being the highest-volume merchants subject to higher security risk. Any merchant that suffers a credit card data security breach, regardless of transaction volume, is automatically elevated to Level 1. Most merchants at A&M-San Antonio are Level 4.

PCI (or PCI DSS) Standards: Payment Card Industry Data Security Standards are created by the Payment Card Industry Security Standards Council for the purpose of safeguarding sensitive cardholder data. The precise security measures required by a department will vary depending on how credit cards are accepted—in person, over the phone, or on the internet—but all are covered in the PCI DSS.

Program Fees are monthly fees assessed based on the merchant's total monthly net credit card sales. Financial Services will charge the appropriate service account for transactions processed based on information supplied by Visa/MasterCard, Discover, and American Express. Each merchant number is linked to an appropriate account to which charge backs and monthly service charges will be recorded. Monthly service charges are different for each card type. For more information on monthly service charges, please contact Financial Services.

Third-Party Internet providers for hosting internet/web credit card transactions:
The University currently has contracts with TouchNet that meet PCI requirements.

Contact Office

Business Affairs, Financial Services (210) 784-2035