STANDARD ADMINISTRATIVE PROCEDURE

21.01.02.M0.03 Credit Card Collections

Approved September 2, 2008
Revised October 28, 2011
Revised November 4, 2016
Next Scheduled Review: November 4, 2021

Statement and Purpose

Texas A&M University offers departments the convenience of accepting credit cards as payment for goods and services provided. Departments may accept credit card payments over the counter, over the telephone, through the mail, or over the internet. Supplemental information regarding the program can be found at http://fmo.tamu.edu/e-commerce/.

Definitions

Merchant Accounts: 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, with highest-volume merchants are Level 1. Security audit requirements become correspondingly higher with merchant level ranking. Most merchants at Texas A&M University are the lowest rank, 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.

Merchant Fees: monthly fees assessed based on the merchant's total monthly net credit card sales.

Procedures

1. Establishing New Merchant Accounts

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 SAPS.

1.1. Departments that accept credit cards must fill out the New Credit Card Merchant Application and submit to Financial Management Operations (FMO) at campus mail stop 6000. Each department is required to provide FMO a FAMIS account number to which Program Fees will be recorded.

1.2. A PCI Self-Assessment Questionnaire must be completed and submitted to FMO for each credit card merchant setup. See section 3 of this procedure for more information.

2. Refunds

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. In most cases refunds cannot be processed back to the originating card more than 180 days after the initial transaction. In rare instances of refunds beyond 180 days, 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 FMO Accounts Payable so that a check can be issued.

3. Credit Card Security

Texas A&M University and the payment card industry take the safeguarding of cardholder 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 department by the bank. **Departments are financially responsible for fines resulting from security breaches that originate from their systems.**

3.1. Before a merchant department may receive credit card payments, it must develop and implement adequate security and internal controls that meet Payment Card Industry Data Security Standards (PCI DSS) requirements and University Rules and SAPs (see 29.01.03.M0.01 *Security of Electronic Information Resources*). All equipment, software, and business processes must comply with current PCI security standards. To provide adequate security, the combined efforts of the business and information technology functions within the department or college are necessary.

3.2. 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 Texas A&M IT Security team prior to implementation. Subsequent changes must be approved prior to implementation.

3.3. In addition to the initial PCI Compliance Questionnaire completed during setup, each merchant is required to complete an annual PCI self-assessment questionnaire.

3.4 Credit card numbers should only be stored electronically as a last resort, and then only in full compliance with the most recent PCI DSS requirements.

3.5 Card data should never be transmitted over end user technologies such as email, texting, instant messenger, and so on.

3.6 Obtain background checks for individuals authorized to have access to cardholder data and assign university PCI training (online) upon hire.

3.7 Ensure that the storage of printed cardholder data (such as merchant copies of receipts or daily batch reports), are secured in a location with access limited to those with legitimate business need. Record retention rules dictate that signed payment receipts records be kept 180 days for chargeback disputes.

3.8 Before engaging with third party vendors who support the transaction process (through software, equipment, hosting, personnel, etc.), the vendor must prove PCI compliance, contractually take responsibility for cardholder security to the extent of their control, and commit to ongoing PCI security compliance.

3.9. Texas A&M IT Security 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. FMO will periodically perform reviews of business procedures to help merchants identify ways to better protect cardholder information. Reviews are also available upon request.

4. Merchant Responsibilities

Merchant departments participating in the credit card program are responsible for complying with all rules and procedures issued by the university, FMO, and the PCI Data Security Standard, including periodic business review and completion of the annual PCI questionnaire. Merchants will provide any reasonable assistance necessary to Texas A&M IT Security in the performance of periodic reviews of credit card-related computer or computer network security. This includes providing IP addresses and network configuration diagrams for use in scanning systems for vulnerabilities. Merchants are responsible for notifying law enforcement, Texas A&M IT Security (if applicable), and FMO in the event of a suspected security breach.

5. Financial Management Operations Responsibilities

FMO is responsible for administering the Texas A&M University credit card program and for ensuring that participating departments are provided updates on all rules, procedures, and security standards. In addition FMO will: coordinate with the merchant bank on the merchant's behalf- including cases of a suspected security breach; distribute and coordinate the preparation of the annual PCI questionnaire by each merchant; work closely with both the merchant and Texas A&M IT Security to ensure that all necessary security procedures

are in place to ensure protection of sensitive credit card data; assess service charges to merchant department accounts for credit card transactions based on information supplied by Visa, MasterCard, Discover, and American Express. Monthly service charges differ for each card type. For more information on monthly service charges, please contact FMO.

6. Texas A&M IT Security Responsibilities

The Texas A&M IT Security team will perform vulnerability scans of PCI computer systems and will require configuration changes to eliminate vulnerabilities. This is both in preparation for and in addition to vendor scans required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. To meet University security needs, the Texas A&M IT Security standards may be stricter than the PCI requirements. Texas A&M IT Security is responsible for approving the configuration of merchants' PCI computer systems.

7. Required Training

Merchant staff who answer questions on the annual PCI questionnaire or who have access to cardholder data, including IT staff who support payment systems, are required to complete an online PCI Security training course. Annual refresher courses are also required. The department is responsible for providing sufficient training to volunteers based on the types of transactions volunteers may process. For more information on available training, please see the Texas A&M Credit Card Merchant Resources website.

8. Disposal of Surplus or Nonfunctional Equipment

When a department no longer needs a particular device to swipe or read credit cards, that card-reader must be returned to FMO for disposal.

Related Statutes, Policies, or Requirements

Supplements System Policy 21.01, *Financial Policies, Systems and Procedures* and System Regulation 21.01.02, *Receipt, Custody, and Deposit of Revenues*.

University SAP 29.01.03.M0.01, *Security of Electronic Information Resources*

University SAP 21.01.02.M0.01, *Online Payments*

Texas A&M Information Security Controls Catalog

Appendix

Payment Card Industry Data Security Standards (PCI DSS)

Texas A&M Credit Card Merchant Resources

Forms

New Merchant Service Request (PDF)

Contact Office

For clarification or interpretation contact Financial Management Operations (FMO) at (979) 845-8118 or (979) 845-6707.