

STANDARD ADMINISTRATIVE PROCEDURE

21.01.02.M0.03 Credit Card Collections

Approved September 2, 2008

Next Scheduled Review: September 2, 2011

Statement and Purpose

Texas A&M University offers University 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://finance.tamu.edu/fmo/apcc/default.asp>.

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 Texas A&M 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.

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. Departments that accept credit cards must fill out the [New Merchant Service Request](#) and submit to Financial Management Operations (FMO) at campus mail stop 6000. Each department is required to provide FMO an account number to which charge backs and monthly service charges will be recorded.

- 1.1. A [PCI Compliance 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 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 (see [29.01.99.M1: Security of Electronic Information Resources](#)). 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 Computing Information Services ([CIS](#))

[Network Security Team](#) prior to implementation. Subsequent changes must be approved prior to implementation.

- 3.3. All equipment and software must comply with current PCI security standards. Non-compliant equipment or software must either be reconfigured or replaced.
- 3.4 Computer or computer network security and internal controls should include, but are not limited to:
 - 3.4.1 Installation and maintenance of a firewall configuration to protect cardholder data.
 - 3.4.2. Protection of stored cardholder data through encryption. Store as little cardholder data as necessary.
 - 3.4.3. Encrypted transmissions of cardholder data. Credit card data submitted via e-mail should never be accepted.
 - 3.4.4. The use of regularly updated antivirus software or programs.
 - 3.4.5. Development and maintenance of secure systems and applications.
 - 3.4.6. The restriction of computer and physical access to cardholder data to authorized personnel. Credit card information stored on a computer must be password protected and credit card information must be encrypted. Credit card information should be located on a drive or server with very limited access.
 - 3.4.7. Assignment of a unique user ID to each person with computer access.
 - 3.4.8. Tracking and monitoring of all access to network resources and cardholder data.
 - 3.4.9. Regularly tested security systems and processes, in accordance with the most current Best Practices and PCI Standards.
- 3.5. Business process security and internal control features should include, but are not limited to:
 - 3.5.1. Obtaining background checks for individuals authorized to have access to cardholder data, in accordance with PCI DSS items 12.7.
 - 3.5.2. Requiring that clerks conducting credit card transactions in person always keep the credit card within the customer's sight.
 - 3.5.3. Accepting credit card transactions for no more than the amount of the purchase.
 - 3.5.4. Confirming that the amount entered into the credit card machine agrees with the purchase amount.
 - 3.5.5. Assuring that the credit card expiration date is not included on the receipt.
 - 3.5.6. Ensuring that only the last 4 digits of the credit card number prints on the receipt copy given to the customer. Departments must ensure that machines meet this requirement. Departments must

notify FMO at 845-5209 or 845-8118 if a machine is not in compliance.

- 3.5.7. Requiring that third-party vendors with access to sensitive cardholder data be contractually obligated to comply with PCI security standards.
- 3.5.8. Ensuring 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 records be kept FY+3.
- 3.5.9. Requiring that the authorization of access to keys for file cabinets containing cardholder data be restricted to personnel who have a business need to such access.
- 3.5.10. Avoiding storage of cardholder data on portable computer devices or storage media.

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

3.7. CIS 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 FMO and with all PCI Data Security Standards, including periodic business review and completion of the annual PCI questionnaire. Merchants will provide any reasonable assistance necessary to CIS 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, CIS Network Security (if applicable – see [SAP 29.01.99.M1.09: Information Resources – Incident Management](#)), 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 CIS 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. CIS Network Security Group Responsibilities:

The CIS Network Security Group will perform vulnerability scans of PCI computer systems and will require configuration changes to eliminate vulnerabilities. (See [SAP 29.01.99.M1.01: Guidelines on Network Scanning](#)) This is both in preparation for and in addition to vendor scans that are required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. In order to meet University security needs, the CIS Network Security Group standards may be stricter than the PCI requirements. The CIS Network Security Group is responsible for approving the configuration of merchants' PCI computer systems.

7. Required Training:

All departmental staff who will be involved in the acceptance of credit card data, including IT staff who support systems that process credit card data, are required to complete an on-line PCI Security training course before being allowed to handle credit card information. Periodic refresher courses will also be 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

University Rule [29.01.99.M1](#) (Security of Electronic Information Resources)

Standard Administrative Procedure [21.01.02.M0.01](#) (Online Payments)

Standard Administration Procedure [29.01.99.M1.01](#) (Guidelines on Network Scanning)

Standard Administration Procedure [29.01.99.M1.09](#) (Incident Management)

[AggiE-Pay](#) informational website.

This SAP supplements: [System Policy 21.01, Financial Policies, Systems and Procedures](#) and [System Regulation 21.01.02, Receipt, Custody, and Deposit of Revenues](#).

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 rule clarification or interpretation contact Financial Management Operations (FMO)
(979) 845-8118 or (979) 845-6707