21.01.02.R0.01 Credit Card Collection

Revised October 3, 2023
Next Scheduled Review: October 3, 2028

Procedure Summary

East Texas A&M University offers university departments the convenience of accepting credit cards in payment for goods and services provided. Departments may accept credit card payments over the counter, over the telephone, or over the Internet.

This procedure establishes the process for accepting credit card payments and ensuring the adherence to Payment Card Industry Data Security Standards (PCI DSS) as required by System Regulation 21.01.02.

Procedures and Responsibilities

1 NEW MERCHANT ACCOUNTS

Departments that decide to accept credit cards must make a direct request to Financial Management. Departments should contact Financial Management to determine the best solution to their credit card collection needs. Financial Management will establish a new merchant account through the credit card processor on the department's behalf. New merchant account activation typically takes three weeks from the time Financial Management receives the request.

1.1 For departments that plan to accept cards in person, Financial Management will acquire the necessary hardware for installation to ensure compatibility with current systems. In certain circumstances, it may be necessary for the department to purchase the hardware themselves. Depending on placement, this equipment may require work orders for telecommunications or AC power accommodations.

1.2 Departments that want to receive credit card payments in instances where the card is not present (such as over the phone, by fax, or online) need to provide complete information to Financial Management to establish an e-commerce site and discuss the setup process. Contact Financial Management at (903) 886-5056 OR (903) 886-5032.

2 CREDIT CARD SALES

Credit card sales should be recorded like any other sale. Customers should be given receipts verifying payment for purchases unless the nature of the transaction precludes the issuance of a receipt (mail and telephone acceptance) or an exception is granted by the Associate Vice President for Finance and Administration / Controller.

2.1 To process sales for walk-in customers presenting an acceptable credit card, the card should be run through a point of sale (POS) device 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 Management.

2.2 To process transactions in which the card is not physically present (such as telephone, fax, or mail orders), departments should contact Financial Management 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 Management.

2.3 Processing "card not present" payments through TouchNet or 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:

Customer Name
Credit card account number
Expiration date of the credit card
Three digit customer verification value (CVV) on the back of the card

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

3 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. 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 through Mane Market so that a check can be issued. Please contact Accounts Payable at 903-886-5048 or 903-886-5061 or mane.market@tamuc.edu for assistance

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 on a daily basis by a department deposit. This report should break down the Visa/MasterCard, Discover, and American Express totals. If the department has 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

The University 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.

5.1 Before a department can begin to receive credit card payments, they must implement adequate security and internal controls that meet PCI DSS requirements. To ensure adequate security, the department must request set up and approval from both the Center for Information Technology Excellence and Financial Management departments. Departments will be required to complete a Device Request Form. Staff members who will be handling credit card data must complete a Statement of Responsibility and will be provided with information on responsibilities for PCI compliance. The necessary forms and other PCI information are located online at http://www.tamuc.edu/admissions/tuitionCosts/bursar/pciStandards.aspx

5.2 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 Center for Information Technology Excellence prior to implementation. Contact 903-468-6000 for placing a work order.

5.3 All equipment and software, including POS must comply with current PCI security standards. No equipment will be allowed to be used unless approved by Financial Management. No software including POS software will be allowed to be used unless approved by the Information Security Officer and Financial Management. Non-compliant equipment or software must either be reconfigured or replaced.

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

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

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

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

5.4.4 Use and regularly update antivirus software or programs.

5.4.5 Develop and maintain secure systems and applications.

5.4.6 Restrict computer and physical access to cardholder date to authorized personnel.

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

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

5.4.9 Regularly test security systems and processes, in accordance with the most current Best Practices and PCI Standards.

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

5.5.1 Individuals will be instructed on processing card transaction in accordance with PCI DSS items 12.7 and will be required to complete A&M System required training for PCI and Basic Cash handling.

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

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

5.5.4 The amount entered into the credit card machine must agree to the purchase amount.

5.5.5 Only the last 4 digits of the credit card number should print on the receipt copy given to the customer. Please make sure your machine is in compliance with this. Notify Financial Management at 903-886-5994 if your machine is not in compliance.

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

5.5.7 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.

5.5.8 Only authorized personnel should have access to keys to file cabinets containing cardholder data.

5.6 For merchant entities, in addition to the initial PCI Compliance Questionnaire completed during setup, completion of an annual PCI self-assessment questionnaire is required. Different versions of the self-assessment questionnaire are available based on the manner in which credit card payments are accepted. Please contact Financial Management for assistance.

5.7 Center for Information Technology Excellence 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 Management is available to conduct reviews of business procedures to help departments identify ways to better protect cardholder information.

6 DEPARTMENT RESPONSIBILITIES

Departments participating in the credit card program are responsible for complying with all rules and procedures issued by Financial Management and all PCI Data Security Standards, including periodic business review and completion of the annual PCI questionnaire. Departments will provide reasonable assistance necessary to Center for Information Technology Excellence 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 required to maintain a detailed log of individuals accessing credit card data. Departments are responsible for notifying Center for Information Technology Excellence and Financial Management in the event of a suspected security breach.

7 FINANCIAL MANAGEMENT OPERATION RESPONSIBILITIES

Financial Management is responsible for administering the university's credit card program and for ensuring that participating departments are kept current on all rules, procedures and security standards. Financial Management will coordinate with the merchant bank on behalf of the department for all data security issues, including any suspected security breach. Financial Management will distribute and coordinate the preparation of the annual PCI questionnaire to each merchant entity. Financial Management will work closely with both the department and Center for Information Technology Excellence to ensure that all necessary security procedures are in place to ensure protection of sensitive credit card data.

8 CENTER FOR INFORMATION TECHNOLOGY EXCELLENCE

8.1 Center for Information Technology Excellence 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 Center for Information Technology Excellence standards may be stricter than the PCI requirements, to meet campus needs.

8.3 Center for Information Technology Excellence is responsible for approving the configuration of all network equipment on which credit card payments may be processed to insure PCI compliance.

9 REQUIRED TRAINING

All departments' staff, including student workers and graduate assistants who will be involved in the acceptance of credit card data, including CITE 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. Annual refresher courses will be required.

10 DISPOSAL OF SURPLUS OR NONFUNCTIONAL EQUIPMENT

Center for Information Technology Excellence is responsible for the disposition of any surplus or non-functioning network equipment on which credit card payments may be processed. This is to ensure that all sensitive information is removed from the POS device.

Related Statutes, Policies, or Requirements

PCI Security Standards Council

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

University Procedure *21.01.02.R0.02 Credit Card Information Receipt, Custody, and Security Procedure*

University Procedure *29.01.09.R0.02 Information Technology Risk Assessment*

Definitions

Merchant, for the purposed of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder date on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts cards for monthly billing, but also is a service provider if it hot merchants as customers.

Merchant Accounts or Merchant Entities 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. Merchant Accounts must be in place before credit cards can be accepted, and accounts can be revoked for failure to comply with the processor's guidelines. University departments or offices with such accounts are 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 the University are Level 4.

PCI (or PCI DSS) Standards: Before a department can receive credit card payments, they must develop and implement adequate security and internal controls as required by Payment Card Industry Data Security Standards (PCI DSS) and University rules. The goal of these security standards is the safeguarding of 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 Management 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 service 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 Management.

Marketplace U Store is a self-contained online store allowing the university department to create a store front, establish for department specific setting, and perform all online store activity such as order fulfillment and reporting. It is a PCI compliant way to take online payments.

Marketplace U Pay is a payment application that utilizes an existing Business Application or website to provide a PCI compliant way for a user to take online payments. U-Pay focuses on payment collection and reporting.

Third Party Internet providers for hosting internet/web credit card transactions: The University currently has contract with the following: TouchNet and Sallie Mae that meet PCI requirements.

Revision History

Approved September 15, 2008
Revised March 31, 2014
Revised November 7, 2024 (University Name Change)

Contact Office

Financial Management
903.886.5991