Credit Card Procedures and Policies

Texas A&M Health Science Center offers university departments the convenience of accepting credit cards in payment for goods and services provided. All University departments wishing to accept credit cards for payment must comply with University procedures and Payment Card Industry (PCI) Data Security Standards.

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 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.

- PCI (or PVI 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. Finance and Administration will charge the appropriate service account for transactions processed based on information provided by Visa/MasterCard, Discover and American Express. Monthly service charges are different for each card type.

Procedures

- Account Setup
  Contact Pat Gilbert (436-9232) in Finance and Administration (F&A) to determine the best solution to your credit card transaction needs.
If you plan on accepting cards in person, you must complete all pages of the New Location Request form, including sections on hardware needs. In certain circumstances, it may be necessary to purchase or lease equipment from the credit card processor. Depending on the equipment's placement, you may require work orders for telecommunications or AC power accommodations.

F&A will require a list of individuals that will be handling credit cards sales; these individuals will need to complete the online PCI training and supply F&A with a transcript prior to the release of the merchant number.

New merchant account activation typically takes 3 weeks from the time the forms are received by F&A.

- **Card Processing, Daily Close out, and Deposit Procedures**
  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 Associate Vice President and Assistant Controller.

- 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 card must be kept within the customer's sight and the CVV code must never be copied or stored. Any exceptions must be approved by the Associate Vice President and Assistant Controller.

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

- For credit card sales, the credit card batch settlement statement and corresponding bill slips should be scanned with the IDT/Cash Deposit Form and dropped into Laserfiche folder 9.0 In-Boxes\A/R & Deposits. The IDT/Cash Deposit form should break down the Visa/MasterCard, Discover, and American Express amounts on separate lines. Credit Card terminal should be settled daily; deposits should be submitted daily.

- Merchants are responsible for reconciling credit card deposits to their FAMIS statements.

- **Charges Related to Credit Cards**
  In addition to terminal, printer, and pin pad device expenses, each type of credit card charges a transaction fee(s). These are also known as surcharges, discount fees, or settlement fees. Departments accepting credit cards for payment are responsible for all fees associated with their acceptance. As of February 14, 2012, the prevailing base fees
(exclusive of equipment fees) are:
Visa/MasterCard - 1.79% - 2.19%
American Express - 3.25%
Discover – 1.55%

• **Equipment Replacement/Disposal**  
  When you no longer need a particular device to swipe or read credit cards. That device must be returned to F&A for disposal. Notify F&A at 436-9232 if you have a device needing to go to surplus. This allows F&A to insure that all sensitive information is removed from the device prior to disposal.

• **Credit Card Security Compliance**  
  Texas A&M Health Science Center takes credit card security very seriously. All departments who accept credit cards as a form of payment must comply with security rules established by the Payment Card Industry Security Standards Council and our card processor Global Payments. All department 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.

• **PCI-DSS**  
  Payment Card Industry (PCI)  
  Data Security Standards (DSS)  
  Established by VISA and MasterCard - endorsed by all major issuers of credit cards  
  Purpose was to create and maintain common industry security requirements.

• **Why does TAM HSC have to follow PCI Standards?**  
  It is mandated by credit card companies - we must adhere to standards or we can lose the ability to accept credit cards for payment

  It is intended to help protect cardholders against fraud and identity theft.

  Penalties for a security breach can be severe. Monetary finds can be very large and security breaches can create very bad publicity for the University.

• **What if we have a Security Breach?**
If a security breach is confirmed or suspected -

Contact F&A immediately

F&A will work with department to determine extent of breach

The University may need to contact cardholders, credit card companies, or law enforcement authorities.

• **Departments will perform and be held responsible for the following:**
  Departments involved with the acceptance/processing of credit cards for payment of goods and services must design adequate processes to ensure the following:
  A. Approval must be obtained from F&A prior to entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method or technology used (POS devices, e-commerce, etc).
  B. Users must comply with PCI standards
  C. You must follow established procedures to ensure that cardholder information is handled and stored securely. This applies to all transactions regardless of the type of transaction (phone, in person, mail, web, etc).
  D. Credit Card numbers can only be transmitted by secure means. This means that insecure transmission methods such as email, fax, or campus mail are not allowed.
  E. Credit card information (full account number, expiration date, PIN, or validation code) must not be stored in any University system, personal computer or email account.
  F. The entire credit card number must not be printed on the customer copy of sales receipts.
  G. Documentation containing full credit card numbers must be stored in a secure environment such as a locked drawer or safe with limited access.
  H. Stored credit card information will be retained according to an approved document retention policy. Media used for credit cards must be destroyed when retired from use and hardcopy must be shredded prior to disposal.
  I. Background checks will be performed prior to hiring for any positions with access to stored cardholder information.
  J. Users must agree in writing not to disclose or acquire any information concerning a cardholder’s account without the cardholder’s consent.
  K. Users must agree to follow ALL PCI standards regarding credit card information.
  L. Users must complete annual credit card security training.

Departments not in compliance with these procedures may lose the ability to
function as a credit card merchant.

Employees in violation of these procedures may be subject to a range of sanctions including loss of computer network access, disciplinary action or legal sanctions. Certain violations may constitute criminal offenses under local, State or Federal laws. The University will exercise its responsibility to report such violations to the appropriate authorities.

• **F&A will perform the following functions:**
  A. Administer the process for obtaining new merchant numbers
  B. Distribute and coordinate the preparation of the annual PCI Self-Assessment Questionnaire.
  C. Provide annual training on secure storage and disposal of credit card information via online training on Train Traq.
  D. Provide guidance for completion of the annual Self-Assessment Questionnaire.

• Technology Services will perform the following functions:
  A. Review and approve implementation of any changes in technology and payment gateways used for processing of credit card data.
  B. Prepare and maintain protected network segments to properly isolated credit card transactions.
  C. Conduct periodic assessments of security controls in place to protect PCI related technology implementations - including but not limited to periodic network-based vulnerability scans.
  D. Provide guidance for completions of the annual Self-Assessment Questionnaire.