OP 62.06: Payment Card Processing by University Departments

DATE: August 20, 2012

PURPOSE: The purpose of this Operating Policy and Procedure (OP) is to establish policy and procedures for acceptance of payment cards by university departments for sales and services.

REVIEW: This OP will be reviewed in July of even-numbered years by the managing director of Accounts Receivable with recommended revisions forwarded through administrative channels to the chief information officer (CIO), the associate vice president for financial affairs/controller (AVPFAC) and the vice president for administration & finance and chief financial officer.

POLICY/PROCEDURE

1. General Policy

Texas Tech University only accepts payment cards either physically via a point of sale terminal or online via a web application.

a. Payment Card Processor–All payment card transactions must go through TTU’s payment card processor, Global Payments.

b. Methods Of Processing–Texas Tech University accepts payment cards either physically or online. Merchants that want to begin processing payment cards should use one of the following TTU-approved processing methods:

(1) Physically–This is done through a point of sale terminal procured though TTU’s payment card processor.

(2) Online–This is done either through an application provided internally by TTU or a hosted solution by a Payment Card Industry Data Security Standards (PCIDSS)-compliant third-party vendor approved by the CIO and AVPFAC.

c. Acceptable Vendors–Only PCIDSS-compliant vendors may be used. All software contracts and purchase orders must include non-disclosure and/or confidentiality statements. Proof of compliance must be:

(1) In writing from the vendor or other credible source, such as Visa; and

(2) Sent to the Credit Card Operations department in Accounts Receivable.
For further information, contact the Credit Card Operations department in Accounts Receivable at 806.742.3271 or at http://www.depts.ttu.edu/fa/departments/ar/ccOperations.asp.

d. Special Needs—For short-term special circumstances where TTU departments need to process payment cards on a temporary basis, contact the Credit Card Operations department in Accounts Receivable at 806.742.3271 for assistance.

2. Establishing And Maintaining Payment Card Services

   a. Establishing Accounts

      Merchant IDs will not be issued until the merchant meets all of the following requirements:

      (1) Complete and submit to the Credit Card Operations department in Accounts Receivable:
          - Payment Card Merchant Request Form (Attachment A);
          - Payment Card Merchant Risk Assessment Survey (Attachment B);
          - Payment Card Merchant Request To Use A Hosted Solution, if applicable (Attachment C);
          - Policy Attestation Form (Attachment E);
          - Xtender Agreement (Attachment F); and
          - PCIDSS Self-Assessment Questionnaire (see 4.g.)

      (2) Complete the required training (Attachment D)–Training for all departmental staff involved in payment card processing is required.

   b. Maintaining Accounts

      Merchant IDs may be revoked if the merchant does not meet all the following requirements:

      (1) Complete the PCIDSS Self-Assessment Questionnaire annually or upon any change to the hardware, software, or payment card processing methodology and submit to the TTU IT security officer;

      (2) Complete required training annually (Attachment D);

      (3) Complete Policy Attestation Form annually (Attachment E); and

      (4) Continued compliance with this OP, PCIDSS, and TTU IT security policies

3. Authority And Responsibility

   a. The Accounts Receivable department is responsible for:

      (1) Issuing a payment card merchant ID and for overseeing the policies and procedures on payment processing;

      (2) Negotiating payment card processing and related services on behalf of any TTU department;
(3) Performing monthly reconciliation on the bank account or payment card clearing account, as applicable, to which payment card receipts are credited;

(4) Determining if the charges have been assessed against the bank account in accordance with the pending procurement document(s) during the account reconciliation process;

(5) Making the appropriate accounting entries to cause the charges to be reflected in the financial accounting records, upon determining that the charges have been incurred;

(6) Resolving discrepancies related to payment card charges with the TTU payment card processor and, if necessary, soliciting the assistance of the merchant to aid in the resolution of the issue(s);

(7) Preparing journal vouchers to charge each department for the discount fee incurred by the respective department for its payment card sales. The discount fee and related fees and expenses are variable and subject to periodic re-negotiation;

(8) Verifying that all merchants are in compliance with TTU policies regarding protecting cardholder data; and

(9) The revocation of a merchant ID that fails to comply with the PCIDSS and/or this OP

b. The Information Technology Division is responsible for:

(1) The operations and maintenance of the TTU data networks, as well as the establishment of IT security policies and standards in compliance with PCIDSS, federal, state, and local regulations;

(2) Developing and maintaining a TTU PCIDSS data network for the hosting of computers, servers, and online storage engaged in processing or storage of payment card transactions;

(3) Assisting any merchant in assessing its payment card processes, applications, and migration to a PCIDSS-compliant solution for the processing of payment cards; and

(4) Verifying that all merchants are in compliance with the PCIDSS requirements

c. The merchant is responsible for:

(1) Continued compliance with this OP, PCIDSS, and TTU IT security policies in order to continue processing payment card transactions;

(2) Completing and submitting a PCIDSS Self-Assessment Questionnaire for every merchant ID assigned to them and for certifying their compliance with this OP and all other related policies. PCIDSS Self-Assessment Questionnaires must be submitted annually and after any major change or upgrade to the software, hardware, or payment card processing methodology, whichever occurs first.

(3) Developing a system and procedure to monitor and analyze security alerts and information and distribute these alerts to the appropriate personnel;

(4) Verifying that their software, hardware, applications, or other devices, products, etc., and associated processes for processing payment cards meets PCIDSS requirements
(assistance from the Accounts Receivable department and the TTU IT Division may be needed);

(5) Maintaining and safeguarding all payment card processing equipment according to the PCIDSS standard. The equipment must be able to produce receipts (merchant and/or customer) that mask all but the last four digits of the cardholder’s card number.

(6) Contacting the payment card processor regarding defective payment card processing equipment. The merchant should return the equipment directly to the payment card processor, provided the payment card processor has instructed the merchant to return the equipment. The merchant should obtain a comparable replacement directly from the payment card processor.

(7) Contacting the Credit Card Operations department in Accounts Receivable at 806.742.3271 to relocate its purchased payment card processing equipment or dispose of the equipment in accordance with the PCIDSS standard and relevant TTU O Ps when the merchant discontinues the acceptance of payment cards. Purchased equipment should not be returned to the payment card processor. If a merchant leases the equipment, it should be returned to the current leasing company upon discontinuing acceptance of payment cards; otherwise, the department will be responsible for ongoing equipment charges. Before any payment card processing equipment is transferred to another department or returned to the leasing company, all payment card data must be securely removed. If the equipment will be disposed of, all payment card data must be securely removed or the storage device must be destroyed to prevent unauthorized access to the data.

(8) Maintaining a record retention and disposal policy to keep information storage to a minimum, ensuring that information will be used for business and regulatory purposes only, and that information will comply with the Xtender Agreement (Attachment F) regarding the imaging of payment card numbers and/or information and OP 52.04, Information Technology (IT) Security, section 3, regarding protection of all data and information resources. Contact the university archivist at the Southwest Collection/Special Collections Library at 806.742.3749 for records retention guidance.

4. Definitions

a. Payment Card–A payment card supports cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and charge cards.

b. Merchant–Each department processing payment card transactions is referred to as a merchant.

c. Merchant ID–A merchant ID is a unique number used to identify the department and card type. Accounts Receivable will request the required merchant identification number from the payment card processor and provide it to the merchant.

d. Payment Card Industry Data Security Standards (PCIDSS)–PCIDSS is a single approach to safeguarding sensitive data for all types of payment cards. The standards are a result of collaboration between Visa and MasterCard and are designed to create common industry security requirements. To download the PCIDSS go to http://www.pcisecuritystandards.org/

e. Payment Card Application–Payment card applications can be hardware, software, or a combination of hardware and software that aid in the processing of payment cards. Examples
include point of sale (POS) devices, web applications/forms that collect or process payment cards, or third party systems that process payment card transactions.

f. Payment Card Processor–A payment card processor offers merchants online services for accepting payment online, including credit card, debit card, direct debit, bank transfer, and real-time bank transfers.

g. PCIDSS Self-Assessment Questionnaire–The PCIDSS Self-Assessment Questionnaire is a validation tool intended to assist a merchant and service provider(s) in self-evaluating its compliance with PCIDSS. To download the PCIDSS Self-Assessment Questionnaire, go to http://www.pcisecuritystandards.org/

h. TTU PCIDSS Data Network–The TTU PCIDSS data network is a secure, firewalled network within the Texas Tech’s TTUNet network, developed according to the PCIDSS standard, for the hosting of computers, servers, or storage that process payment card transactions and data.

Attachment A: Payment Card Merchant Request Form
Attachment B: Payment Card Merchant Risk Assessment Survey
Attachment C: Payment Card Merchant Request To Use A Hosted Solution
Attachment D: Training
Attachment E: Payment Card Industry – Data Security Standards (PCIDDS) Policy Attestation
Attachment F: Xtender Imaging Payment Card Industry Data Security Standards (PCIDSS) Compliance Policy Agreement