TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 62.06: Payment Card Processing by University Departments

DATE: October 8, 2019

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 odd-numbered years by the Managing Director of University Financial Services with recommended revisions forwarded through administrative channels to the Chief Information Officer, the Assistant Vice President and Controller and the Vice President for Administration & Finance and Chief Financial Officer.

POLICY/PROCEDURE

1. General Policy

a. Payment Card Processor. All payment card transactions must go through Texas Tech University's (TTU) payment card processor, currently Bank of America (BAMS).

b. Methods of Processing. TTU processes payment cards both physically and online. Merchants that want to begin processing payment cards, *must* use one of the following TTU-approved processing methods:

(1) Physically
This is done through a point of sale terminal procured through TTU's payment card processor. If a PCI SSC validated P2PE solution is available, it **must** be used unless an exception is granted by the TTU Office of the CIO.

(2) Online
This is done through TTU's online e-commerce solution Touchnet Marketplace. Any exception to this MUST be reviewed and approved by both University Financial Services (UFS) and the TTU Office of the Chief Information Officer (CIO).

(3) Phone
If accepting a payment card over the phone, secure processes must be followed in the way that data is handled and processed for payment. These processes need to be reviewed by UFS to ensure all appropriate security standards are met.

c. Acceptable Vendors. If using a third party software, the software must connect through the University e-commerce solution Touchnet Marketplace. Any exception to this must be reviewed and approved by both UFS and the TTU Office of the CIO. Only PCI DSS-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) a written agreement from the service providers acknowledging they are responsible for the security of cardholder data the service providers possess and
(2) sent to the Credit Card Operations Department in UFS.

d. Credit Card Equipment Loans. Available from UFS if you have a one-time or temporary event in which you need the use of credit card equipment. UFS requires a minimum of 3 days written notice. It is in your best interest to contact UFS as early as possible to reserve the equipment and confirm that it is not already scheduled for a different event or department. For credit card equipment loans, submit the completed application (Credit Card Equipment Loans) to UFS at financial.services.receptionists@ttu.edu.

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 UFS:
- TTU Merchant Application & Update Form,
- Policy Certification,
- Xtender Agreement, if needed
- Exception form, if needed (contact UFS),
- Data Flow Diagram, if needed (contact UFS),
- PCI DSS Awareness online training

b. Maintaining Accounts. Merchant IDs may be revoked if the Merchant does not meet **all** of the following requirements. UFS will reach out to all merchants during the Fall of every year to request updates on each of these in order to comply with PCI DSS certification regulations for the University.

(1) Complete the PCI DSS Self-Assessment Questionnaire (SAQ) annually or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Credit Card Operations Department in UFS (contact UFS for assistance with appropriate SAQ to complete),

(2) Complete the TTU Merchant Application & Update as requested by UFS, or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Credit Card Operations Department in UFS,

(3) Complete required PCI DSS Awareness online training annually. Training is required for:

- Any employees who process payment cards or have access to sensitive payment card information received by their department for payment card transactions
- Supervisors of the above employees
- Departmental Business Managers whose department accepts credit card payments
- Others who oversee payment card operations in a department

(4) Complete Policy Certification annually. Required by the same individuals listed in Section 2.b(3) of this OP, *and*

(5) Continued compliance with this OP, PCI DSS, and TTU IT Security Policies.

3. Authority And Responsibility

a. **University Financial Services is responsible for:**

(1) issuing a payment card Merchant ID and for overseeing the policies and procedures on payment processing (UFS requires a minimum of six (6) weeks notice from the date of completing a finalized application, to obtain a set of new merchant ids),

(2) negotiating payment card processing and related services on behalf of any TTU department,

(3) performing monthly reconciliation on the bank account, 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) assisting merchants with resolving discrepancies related to payment card charges with the TTU payment card processor,

(6) 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 re-negotiation periodically,

(7) verifying that all Merchants are in compliance with TTU policies and current PCI DSS financial controls in regards to protecting cardholder data, and

(8) the revocation of a Merchant ID that fails to comply with the PCI DSS 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 PCI DSS, Federal, State, and local regulations,

(2) developing and maintaining a TTU PCI DSS 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 PCI DSS-compliant solution for the processing of payment cards, and

(4) verifying that all Merchants are compliant with the current PCI DSS technical requirements.

c. **The Merchant is responsible for:**

(1) all requirements outlined above in Section 2.b. of this OP,

(2) developing a system and procedure to monitor and analyze security alerts and information and distribute these alerts to the appropriate personnel,

(3) developing and maintaining departmental policy and procedures for physical inspection of payment card equipment, including frequency and methods of inspection and submitting this policy to UFS annually or as requested.

(4) verifying that their software, hardware, applications, or other devices, products, etc. and associated processes for processing payment cards meets PCI DSS requirements - assistance from the UFS and the TTU IT Division may be needed,

(5) maintaining and safeguarding all payment card processing equipment according to the PCI DSS standard. The equipment must be able to produce receipts (merchant and/or customer) that masks 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 UFS to relocate its purchased payment card processing equipment (media) or dispose of the equipment in accordance with the PCI DSS standard and relevant TTU Operating Policies when the Merchant discontinues the acceptance of payment cards. Purchased equipment should 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 on-going equipment charges. Before any payment card processing equipment is transferred to another department or returned to the leasing company, verify all payment card data has been 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 in accordance with OP 10.10, *Records Retention*, to keep information storage to a minimum, that information will be used for business and regulatory purposes only, and that information will comply with the Xtender Agreement regarding the imaging of payment card numbers and/or information and OP 52.04, *Information Technology (IT) Security*. Contact the University Archivist at the Southwest Collection/Special Collections Library at 806.742.3749 for records retention guidance.

(9) responding to card brand chargebacks, disputes, sales draft retrieval requests or other requests from the issuing bank or cardholder within the specified time period providing proper documentation, or determining that the chargeback, dispute or other request is legitimate and should stand as is.

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. UFS will request the required merchant identification number from the payment card processor and provide them to the Merchant.

d. Payment Card Industry Data Security Standards (PCI DSS). PCI DSS 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 PCI DSS go to: http://www.pcisecuritystandards.org/

e. Payment Card Application. Payment Card Applications can be hardware, software, or a combination of hardware and software which aid in the processing of payment cards. Examples include Point of Sale (POS) devices, web applications/forms which collect or process payment cards, or third party systems which 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. PCI DSS Self-Assessment Questionnaire (SAQ). The PCI DSS SAQ is a validation tool intended to assist a Merchant and service provider(s) in self-evaluating their compliance with PCI DSS.
To download the PCI DSS SAQ go to: www.pcisecuritystandards.org/

h. TTU PCI DSS Data Network. A secure, firewalled network within Texas Tech's TTUNet network, developed according to the PCI DSS standard, for the hosting of computers, servers, or storage which process payment card transactions and data.