TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 62.06: Payment Card Processing by University Departments

DATE: July 10, 2023

PURPOSE: The purpose of this Operating Policy/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 April of even-numbered years by the Senior Managing Director of Cash and Credit Management Services and the Chief Procurement Officer with substantive revisions forwarded through administrative channels to the Chief Information Officer (CIO) and the Senior Vice President for Administration & Finance and Chief Financial Officer.

POLICY/PROCEDURE

1. Definitions

a. Payment Card – A payment card supports cashless payment for goods and services.

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

c. Merchant ID – A unique number used to identify the department and Banner FOAP for posting revenue and fees. Cash and Credit Management Services (CCMS) will request the required merchant identification number from the payment card processor.

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 the card brands and are designed to create common industry security requirements. To download the PCI DSS, go to www.pcisecuritystandards.org/.

e. 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.

f. Self-Assessment Questionnaire (SAQ) – Reporting tool used to document self-assessment results from an entity's PCI DSS assessment. There are multiple versions of the SAQ to meet various scenarios, depending on how the organization stores, processes, or transmits cardholder data.

g. TTU PCI DSS Data Network – A secure, firewalled network within Texas Tech's network, that meets PCI DSS standard.

2. Scope and Applicability

a. This policy and its related standards, procedures, and guidelines apply to all TTU data, information systems, activities, and assets owned, leased, controlled, or used by TTU, its agents, contractors, or other business partners on behalf of TTU that are within the scope of the PCI DSS. This policy applies to all TTU employees, contractors, sub-contractors, and their respective facilities supporting TTU business operations, wherever TTU data is stored, processed, or transmitted, including any third party contracted by TTU to handle, process, transmit, store, or dispose of TTU data.

b. Some standards are explicitly stated for persons with a specific job function (e.g., a system administrator); otherwise, all personnel supporting TTU business functions shall comply with the standards. TTU departments shall use this policy and its standards or may create a more restrictive set of policies and standards but not one that is less restrictive, less comprehensive, or less compliant than this policy and its standards.

3. General Policy

a. All payment card activity is subject to the PCI DSS and all applicable TTU Operating Policies, including the TTU PCI Data Security policy.

b. Any office engaged in any form of payment card processing (e.g., POS/swipe or e-commerce) must have the approval of the Office of CCMS prior to engaging in commerce activity. No university department may enter into any contracts or otherwise arrange for payment transaction processing or obtain any related equipment, software, or services without the approval of CCMS and the TTU Office of the CIO. Any contract must be executed in compliance with OP 72.04, Contract Administration, and must be reviewed and approved by the Office of Contract Management.

c. All payment activity must be established within the centralized university banking and accounting environment with receipts deposited through CCMS to the Texas Tech University bank accounts.

d. Texas Tech University's official online payment system is TouchNet. All departments wishing to accept online payment card transactions must use TouchNet unless an exception by CCMS and the Office of the TTU CIO is granted.

e. CCMS is responsible for oversight of campus compliance with the PCI DSS. Any department accepting any payment methods outlined in this policy must submit the appropriate SAQ and other required documents annually and upon request by CCMS.

4. Methods of Processing

a. All payment card transactions must go through the Texas Tech University contracted payment card processor, unless approved by CCMS (these exceptions will be extremely rare).

b. Devices including, but not limited to, mobile devices and computers used for TTU payment transactions, including online e-commerce payments, must be authorized by CCMS and the TTU Office of the CIO.

c. Payments may be accepted physically through point-of-sale terminals procured through TTU's payment processor or other CCMS-approved vendor. A Payment Card Industry Security Standards Council (PCI SSC) validated Point-to-Point Encrypted (P2PE) solution must be used unless an exception is granted by CCMS and the TTU Office of the CIO.

d. Payments may be accepted over the phone. Processes must be followed to ensure data and payment security. These processes need to be approved by CCMS to ensure all appropriate security standards are met. Additional information can be found on the CCMS Resources page.

e. Payments may be accepted through TTU's online e-commerce solution, TouchNet Marketplace, or the TTU-approved POS System, Clover. If a department has a specific business operational need that the approved, official university processing methods cannot meet, the department can apply for an exception. Departments submit their exception request to CCMS. Exception requests will be evaluated and must be approved by both CCMS and the TTU Office of the CIO. As part of the exception evaluation process, CCMS and the TTU Office of the CIO will conduct a full evaluation of proposed equipment, network structure, and remote access privilege use.

f. Payments cannot be accepted through email or fax.

5. Refunding and Fees

a. Refunds from payment card processing will be credited back to the card used during the sale and cannot exceed the original sale amount.

b. Departments are responsible for all costs incurred to set up and process departmental transactions. Processing fees will be deducted monthly from the Banner FOAP provided during set up. In addition, each department is responsible for all hardware, software, installation, and/or maintenance costs needed to maintain the processing environment, including the cost of required security scans, if applicable.

6. Establishing and Maintaining Payment Card Services

a. Establishing Accounts

(1) All requests to engage in any form of payment card processing must be sent to CCMS. To establish a merchant account, the department must submit a TTU Merchant Application and Policy Certification for review and approval by CCMS and the TTU Office of the CIO. Additionally, department personnel must complete PCI DSS awareness online training. Merchant IDs will not be issued until approval is obtained by all levels in both offices. **The review and approval process can take 4–6 weeks.**

(2) Depending on the request, additional forms, such as an Xtender agreement, exception form, data flow diagram, third-party vendor attestation of compliance, SAQ, etc., may be required.

b. Maintaining Accounts

(1) Departments must submit a Pre-SAQ oversight form annually to CCMS. This allows a review of payment processing methods and appropriate assignment of SAQ(s).

(2) Departments must complete the appropriate PCI DSS SAQ(s) each year through the university compliance portal.

(3) Departments must complete the required PCI DSS Awareness training for:

- Any employee who processes payment cards or has 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; and
- Others who oversee payment card operations in a department.

7. Payment Card Security Responsibilities

a. CCMS Responsibilities

(1) Oversight of campus compliance with payment card processing and security regulations. To ensure conformity with university policies and procedures, CCMS has the authority to impose appropriate sanctions up to and including suspension or termination of payment card processing privileges for any TTU department that violates provisions outlined in this policy.

(2) Negotiate payment card processing and related services on behalf of any TTU department.

(3) Review and approve requests for new merchant accounts, processing methods, equipment, and issuing merchant IDs.

(4) Review annual SAQs.

(5) Complete and submit TTU Attestation of Compliance (AOC) for SAQ roll up to the credit card processor.

(6) Review other required departmental documentation annually to meet PCI DSS standards.

(7) Review and communicate PCI DSS requirements to university departments as needed for departments to appropriately comply with requirements.

(8) Maintain a current PCI DSS awareness training for departments.

(9) Reconcile payment card funds deposited in the TTU bank account.

(10) Record payment card fees monthly.

b. Department Responsibilities

(1) Follow all requirements outlined in this OP for establishing and maintaining credit card processing services.

(2) Review and comply with the PCI DSS located online at pcisecuritystandards.org. PCI DSS requirements include, but are not limited to:

(a) Maintain formal, written operational procedures that include transaction processing methods, refund policies, and reconciling procedures. These procedures must be evaluated, updated, and submitted annually (or upon request) to CCMS.

(b) Ensure card information or card-validation (three-digit value printed on the signature panel of a card) is not stored on any TTU computer, database, or server. Cardholder data must be protected by keeping it secure and confidential and only held as needed for business purposes. Once business need has expired, all cardholder data should be securely destroyed (i.e., shredded).

(c) Obtain and maintain documentation of PCI DSS compliance status of any **third-party service providers** directly or indirectly involved in processing credit card transactions (e.g., website hosting services, internet payment gateways, shopping cart providers, etc.) and submit the vendor's current AOC to CCMS annually (or upon request).

(d) For any contract with a **third-party service provider**, ensure language in the contract meets the PCI DSS requirement for a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess.

(e) Maintain updated inventory of equipment.

(f) Perform regular tampering inspections of all payment card equipment.

(g) Maintain all credit card receipts in a secure location for 18 months. All other payment card information should be **securely** destroyed immediately after the business use is complete. Documents uploaded to the university compliance portal annually (e.g., terminal inventory and inspection logs, training certifications, and AOCs) need only be retained for the current compliance year.

(h) Notify CCMS of any change in credit card processing methods.

(i) Respond to chargebacks, disputes, sales draft retrieval requests, or other requests from the issuing bank or cardholder within the specified time period.

(j) Annually or upon request by CCMS:

- Review SAQ types training to identify appropriate SAQ(s) needed;
- Submit required SAQ(s) to CCMS;
- Submit department procedures to CCMS;
- Submit equipment inventory and inspection log to CCMS;
- Submit list of staff identified as needing PCI DSS awareness training;
- Submit Attestations of Compliance (AOC) for third-party vendors; and
- Complete PCI DSS awareness training.

c. Information Technology Division Responsibilities

(1) Operate and maintain the TTU data networks, as well as establish IT security policies and standards in compliance with PCI DSS, federal, state, and local regulations.

(2) Develop and maintain a TTU PCI DSS data network for the hosting of computers and servers engaged in processing payment card transactions, as needed.

(3) Assist merchant departments with PCI DSS technical requirements.

(4) Assist departments accepting payment cards to develop and maintain current network or data flow diagrams as required by the PCI DSS.

(5) Regularly monitor and test networks and review firewalls as required by the PCI DSS.

(6) Review and approve requests for new merchant accounts and processing methods and equipment.

(7) Perform or coordinate any required internal and/or external scans (e.g., vulnerability scans or penetration testing) and submit results to the university acquiring bank as required by the PCI DSS and/or the acquiring bank.