TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Operating Policy and Procedure

HSC OP: 50.37, **Payment Card Processing by TTUHSC Departments**

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to establish the standard institutional procedure for acceptance of payment cards by university departments for sales and services rendered.

REVIEW: This HSC OP will be reviewed on January 1 of every fourth year (E4Y) by the Director of Accounting Services, with recommendations for revisions forwarded through administrative channels to the Vice President for Information Technology/Chief Information Office and the Executive Vice President for Finance and Operations.

POLICY/PROCEDURE:

1. Definitions

a. Payment Card – A payment card supports cashless payments for goods and services (i.e., credit cards, debit cards, charge cards, etc.).

b. Merchant – A TTUHSC business unit that processes payment card transactions (by terminal, eCommerce, or mobile) is referred to as a "merchant." A department may have more than one merchant.

c. Merchant Account Application – An online application used for merchant maintenance including requesting merchants and maintaining/updating merchant information.

d. Merchant Account Application Roles
   i. Payment Card Manager (PCM)
   ii. Secondary Contact
   iii. Finance Contact
   iv. Merchant Users

e. Merchant ID – A merchant ID is a unique number assigned to a merchant by a Payment Card Processor and is used by payment card systems to route money for payment card transactions to the correct bank account(s). A merchant may have more than one merchant ID depending on revenue sources, bank accounts and card types accepted.

f. Payment Card Industry Data Security Standards (PCI DSS) – Standards for safeguarding sensitive data for all types of payment card transactions. The standards are a result of collaboration between Visa and MasterCard and are designed to create common industry security requirements.

g. 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 and web applications/forms that collect or process payment cards.

h. Payment Card Processor – A payment card processor facilitates credit authorization and payment transfer for sales transactions involving payment cards. TTUHSC participates in TTUS system-wide agreements for credit card processing with Fiserv Inc. for Point-of-Sale (POS) terminal and mobile device merchant activity, and with TouchNet for online eCommerce merchant activity. Occasionally, TTUHSC departments identify unique business needs that require credit card processing with vendors other than Fiserv Inc. and TouchNet. These vendors are referred to as third party processors.

i. PCI DSS Self-Assessment Questionnaire – A PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool intended to assist with self-evaluating compliance with PCI DSS.

j. CampusGuard – Third party vendor that provides TTUHSC with PCI DSS services including a portal that provides departments with the tools needed to identify, complete, and manage the appropriate SAQs depending on each department's specific needs. CampusGuard provides guidance and ongoing support as each department completes their SAQs.

k. Third Party Processor – Occasionally, TTUHSC departments identify unique business needs that require credit card processing with vendors other than Fiserv Inc. and TouchNet. These vendors are referred to as third party processors.

2. General Policy

a. Approved Methods of Processing

i. Point of sale terminals or mobile devices issued through approved System credit card processor (Fiserv).

ii. e-Commerce Applications (online/web based) utilizing approved System e-Commerce Payment processing solution (TouchNet).

iii. PCI DSS compliant third-party solutions only with approved exception request.

3. Establishing and Maintaining Payment Card Services

a. Establishing Payment Card Services

i. Point of Sale Processing – Point of sale merchants should utilize equipment issued through the TTUS approved credit card processor (Fiserv) unless otherwise approved.

1) Submit a New Request via the Merchant Account Application and select a "New Terminal" or 'New Mobile" option in the app.

2) New merchant requests are routed for approvals and setup within the Merchant Account Application.

3) Once approved, Accounting Services is responsible for ordering the initial credit card terminal or mobile device.

4) The department/clinic is responsible for setting up the machine and contacting the credit card processor's Help Desk for operating instructions.

ii. e-Commerce Applications (online/web based) – All e-Commerce applications should utilize the TTUS approved eCommerce payment processing solution (TouchNet) unless otherwise approved.

1) Submit a New Request via the Merchant Account Application and select a "New eCommerce" option in the app.

2) New merchant requests are routed for approvals and setup within the Merchant Account Application.

iii. PCI DSS compliant third-party solutions – In some cases, TTUHSC departments identify unique business needs that require credit card processing with vendors other than Fiserv Inc. and TouchNet. These solutions are referred to as third party solutions and require special approval to ensure compliance with procurement, information technology, security and compliance policies and procedures related to credit card acceptance and payment processing.

1) Vendor selection for Third Party solutions should follow normal procurement policies and procedures.

2) A Service Exception Request must be completed and approved by the requesting Department Head, Vice President for Information Technology & CIO (or Assistant Vice President for Information Services), Accounting Services, Institutional Compliance (if applicable) and Institutional Security Officer (if applicable). The Service Exception Request can be accessed under the eCommerce (TouchNet) link at https://hscweb.ttuhsc.edu/it/services.aspx.

3) Proof of PCI DSS compliance from the vendor or other credible source should be submitted with the request.

4) Because these items are not processed through the payment card processor covered under the system wide credit card agreement, the requesting department will be responsible for obtaining Merchant ID(s) from the external party.

b. Maintaining Payment Card Services

Payment card security and compliance is a serious issue for TTUHSC. Non-compliance at the departmental level could have a detrimental impact to the institution including reputational damage to TTUHSC as a result of a data breach or other exposure, large penalties or hefty fines due to non-compliance and merchant processor refusal to process TTUHSC payment card transactions.

Merchants not in compliance with this TTUHSC Operating Policy may have their funds withheld, Merchant ID inactivated, or, other action deemed necessary for TTUHSC to be PCI DSS compliant.

4. Accounting Services Responsibilities

Accounting Services is responsible for the following related to payment card processing for Merchant IDs that have been established through the payment card processor covered under the system wide credit card agreement. This does not apply to any merchant IDs issued as a result of using a third-party solution for which an exception was approved per paragraph 3.a.iii above.

a. Issuing and maintaining merchant IDs

b. Requesting the required merchant identification number from the payment card processor and providing them to the department.

c. Providing a monthly reconciliation of all TTUHSC bank accounts that receive deposits, adjustments, and fees related to payment cards.

d. Making any necessary accounting entries related to payment card disputes and discount fees that are assessed.

e. Resolving discrepancies related to payment card transactions with the credit card processor.

f. Development of the Merchant Account Application as a merchant ID and inventory management app and serve as a database for Information Technology for use in providing annual PCI DSS training and annual completion of merchant SAQs.

g. Act as a liaison between the credit card processor and TTUHSC departments.

h. Notifying IT of any correspondence from credit card processor regarding PCI DDS standards and/or related information requests.

i. In coordination with CampusGuard, select a sample of non-technical departmental responses for validation with in departmental SAQs to ensure accuracy and compliance.

j. In coordination with CampusGuard, develop training materials as needed to support compliance and awareness.

5. Information Technology Responsibilities

a. Establish Information Security policies and procedures in compliance with PCI DSS technical requirements and TTUHSC policies. Please refer to Information Technology policies at https://hscweb.ttuhsc.edu/it/admin/policy.

b. Assist TTUHSC departments in assessing their payment card processes, applications, and devices to ensure, where applicable, migration to a PCI DSS compliant solution for the processing of payment cards.

c. Provide and maintain information technology resources that allows the secure and compliant configuration and use of approved PCI DSScompliant merchant services on the TTUHSC Network.

d. Review and evaluate TTUHSC merchants' compliance with current and applicable PCI DSS technical controls.

e. Maintain Merchant ID information in CampusGuard.

f. Conduct ongoing monitoring and testing of networks, and perform periodic reviews of firewall configurations in accordance with PCI DSS requirements.

g. Ensure coordination and completion of all internal and external vulnerability scans and penetration tests, and submit the results to the TTUHSC's acquiring bank in compliance with PCI DSS requirements specified by the acquiring bank.

h. In collaboration with CampusGuard, select a sample of the technical responses for validation within departmental SAQs to ensure accuracy and compliance.

i. Provide initial and annual PCI awareness training and monitor completion with assistance from CampusGuard.

6. Departmental Responsibilities

a. Continued compliance with this HSC OP, PCI DSS, and TTUHSC IT security and confidentiality policies, and PCI DSS requirements located online at https://pcisecuritystandards.org/ Merchants not in compliance with this HSC OP may have their funds withheld, Merchant ID inactivated, or, other action deemed necessary for TTUHSC to be PCI DSS compliant.

b. Annually, or as requested by Accounting Services, CampusGuard, or Information Technology:

i. Participate in training sessions, including PCI DSS awareness training, and workshops provided by CampusGuard to better understand roles and responsibilities towards data protection, compliance, and determining the appropriate SAQ type(s).
ii. Submit completed SAQ(s) to CampusGuard.
iii. Provide related departmental procedures to Accounting Services or CampusGuard.
iv. Submit an updated equipment inventory and inspection log to Accounting Services.
v. Submit Attestations of Compliance (ACO) for all third-party vendors to Information Technology.

c. Updating merchant information within the Merchant Account Application including correctly identifying people in the following roles:

i. **Payment Card Manager (PCM)**
   1) Manages merchant operations within the department.
   2) Enters and maintains merchant information in the Merchant Account Application.
   3) Serves as the primary contact related to merchant operations.
   4) Oversees setup of terminal, mobile device and eCommerce payment applications.
   5) Establishes and maintains internal controls over merchant operations within the department.
   6) Identifies Merchant Users for required PCI DSS awareness training and enters their names in the Merchant Users list in the Merchant App;
      a) any employee who processes or oversees payment cards (which includes terminals, eCommerce, or mobile) or,
      b) Has access to sensitive payment card information or,
      c) Supervisors of the above employees or,
      d) Departmental Administrators whose department accepts credit card payments or,
      e) Others who oversee payment card operations in a department or,
      f) PCMs, Finance Contacts, and Secondary Contacts who are already Merchant Users. (This group is not required to be entered in the Merchant's User List in the Merchant App.)
   7) Ensures contacts and terminal/device/eCommerce merchant users complete required annual PCI DSS training.
   8) Completes annual the annual Self-Assessment Questionnaire (SAQ).

ii. **Secondary Contact**
   1) Assists PCM with entering and maintaining merchant information in the Merchant Account Application.

iii. **Finance Contact**
   1) Oversees financial reconciliation of payment card transactions

iv. **Merchant Users**
   1) Any employee who processes payment cards (which includes terminals, eCommerce, or mobile). or,
   2) Has access to sensitive payment card information or,
   3) Supervisors of the above employees or,
   4) Others who oversee payment card operations in a department or

5) PCMs, Finance Contacts and Secondary Contacts

d. Update the Merchant Account Application with the make or model, location, and other unique information of payment card devices as needed.

e. Maintaining the security and confidentiality of information in accordance with the applicable HSC Operating Policies and Procedures, including but not limited to:

- HSC OP 52.09, Confidential Information
- HSC OP 52.10, Identity Theft Prevention, Detection and Mitigation Program
- HSC OP 56.01, Acceptable Use of Information Technology Resources
- HSC OP 56.04 Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI)

f. Maintaining and safeguarding all payment card processing equipment according to PCI DSS standard. The equipment must be able to produce receipts (merchant and/or customer) that mask all but the last four digits of the card holder's card number. The department is responsible for contacting the credit card processor's help desk to reprogram their point-of-sale terminal equipment in order to mask the card data on both the customer and merchant receipt copies.

g. Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

h. Verifying that customer receipts generated for eCommerce or other methods do not display the customer's card number.

i. Requesting and maintaining merchant identification numbers from external vendors for all third-party systems and/or processors not covered under the system credit card agreement.

j. Providing Accounting Services with information regarding how third-party processor transactions will be handled through TTUHSC bank accounts. This information is needed for revenue posting and bank reconciliation purposes, and must be provided before Accounting Services will approve any exception request pursuant to paragraph 3.a.iii above. If it is determined that the third-party processor is unable to provide adequate information to allow for efficient and accurate posting and reconciliation of the related transactions, Accounting Services will deny the request to utilize the third-party processor.

k. Providing any documentation required to the credit card companies to settle any and all credit card disputes and customer charge-backs.

l. Supplying Accounting Services with any documentation related to discrepancies found during the reconciliation process and promptly notifying Accounting Services with any changes to the primary contact.

m. For point-of-sale terminals, the department is responsible for contacting the credit card processor's help desk for ordering replacement machines, correcting any problems associated with the credit card terminals, and ordering supplies when necessary.

n. Contacting Accounting Services to relocate its purchased payment card processing equipment or dispose of the equipment in accordance with the PCI DSS standard and relevant TTUHSC OP's when the merchant discontinues the acceptance of payment cards. All purchased terminals should be properly disposed of by returning the equipment to the Credit Card Processor for payment card data removal and disposal of the equipment. Under no circumstances should terminals be sold in surplus. Accounting Services must be notified of any equipment transfers between departments, prior to the transfer taking place, to ensure the equipment is properly programmed. This paragraph applies only to those Merchant IDS

that have been established through the payment card processor covered under the system wide credit card agreement.

o. Maintaining a record retention and disposal policy that keeps information storage to a minimum. Follow HSC OP 10.09, Attachment A Records Retention Schedule, Item 4.2.002: the current fiscal year plus 3 years (FE + 3).

p. Ensuring that information will be used for business and regulatory purposes only.

q. Ensuring that applicable employees have read and understood this policy and those policies referenced herein.

r. Ensuring that it complies with Payment Card Industry Data Security Standards and applicable HSC Operating Policies and Procedures, including but not limited to:

- HSC OP 10.09, Records Retention Schedule
- HSC OP 52.09, Confidential Information
- HSC OP 52.10, Identity Theft Prevention, Detection and Mitigation Program
- HSC OP 56.01, Acceptable Use of Information Technology Resources
- HSC OP 56.04, Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI)

7. Contact Information

a. The credit card processor's help desk phone number can be located on the side of each point-of-sale terminal along with the merchant ID associated with the terminal.

b. Accounting Services can be contacted at merchantID@ttuhsc.edu.

c. Information Technology can be contacted for information pertaining to eCommerce or issues with the TTU System approved eCommerce Payment processing solution (TouchNet) at 806-743-1234 and it.grc@ttuhsc.edu.

d. IT can be contacted for questions regarding SAQs to it.grc@ttuhsc.edu. Additionally, CampusGuard can be contacted for SAQ assistance, workshops, and PCI trainings at info@campusguard.com