TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 50.37, **Payment Card Processing by TTUHSC El Paso Departments**

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

REVIEW: This HSCEP OP will be reviewed on January 1 of every fourth year (E4Y) by the Director of Accounting Services, with recommendations for revisions submitted through administrative channels to the Chief Financial Officer and Assistant Vice President for Information Technology/Chief Information Officer by January 31.

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 – 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.

   d. Payment Card Industry Data Security Standards (PCI-DSS) – PCI-DSS is a single approach to 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. 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 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. PCI-DSS Self-Assessment Questionnaire—the PCI-DSS Self-Assessment Questionnaire 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 Self-Assessment Questionnaire, go to http://www.pcisecuritystandards.org.

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

2. **General Policy**

a. Approved Methods of Processing

i. Point of sale terminal.

ii. e-Commerce Applications (online/web based).

iii. PCI-DSS compliant third party solutions for processing eCommerce transactions (With approved exception request only – See paragraph 3.a.iii below).

NOTE: All e-Commerce applications must utilize the Texas Tech University (TTU) System e-Commerce Payment processing solution (Touchnet) unless otherwise approved.

3. **Establishing and Maintaining Payment Card Services**

a. Establishing Payment Card Services

i. Point of Sale Processing

1. Complete the Merchant ID Information Form (Attachment A). A separate form for each new merchant ID request is required. Once the form(s) are completed, submit them to the Banking and Receivables Accountant in the Accounting Services department.

2. Accounting Services is responsible for obtaining all necessary ID numbers, setting up accounts with the credit card processor, and ordering the initial credit card terminal for those merchant IDs established through the payment card processor covered under the system wide credit card agreement.

3. Upon receiving the ordered terminal(s), 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)

1. An e-Commerce Service Request must be submitted for all e-Commerce applications. The request can be accessed at https://www.ttuhsc.edu/it/is/paws/ecommerce.aspx.

2. All e-Commerce service requests and applications must be 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).

3. If the e-Commerce request requires a new merchant ID, complete the Merchant ID Information Form (Attachment A). A separate form for each new merchant ID request is required. Once the Merchant ID form(s) are completed, submit them to Accounting Services at accountingelp@ttuhsc.edu.

4. All e-Commerce applications must utilize the Texas Tech University System eCommerce Payment processing solution (TouchNet) unless otherwise approved. See PCI-DSS compliant third party solutions for processing eCommerce transactions of this section for more information.

5. Please see HSCEP OP 56.01, Use of Information Technology Resources (including but not limited to sections 1.4.20 and 9.5) for more information regarding the development of e-commerce web applications.

iii. PCI-DSS compliant third party solutions for processing eCommerce transactions

1. In some cases, consideration may be given to the use of a PCI-DSS compliant third party solution for processing eCommerce transactions, which are not processed through the payment card processor covered under the system wide credit card agreement.

   An eCommerce 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 eCommerce Service Exception Request can be accessed at http://www.ttuhsc.edu/it/is/paws/ecommerce.aspx.

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

   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 the Merchant ID from the external party.

b. Maintaining Payment Card Services

4. Merchant ID's may be revoked if the merchant does NOT follow the TTUHSC El Paso Operating Policies and Procedures related to security and confidentiality, information technology, and finance and administration.

5. 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 as well as providing oversight and enforcement for the policies and procedures related to payment processing, excluding eCommerce and any merchant IDs issued as a result of a third party solutions for which an exception was approved per paragraph 3.a.iii above. This includes the revocation of any merchant IDs that fail to comply with this policy.

   b. Requesting the required merchant identification number from the payment card processor and providing them to the merchant upon approval of submitted requests.

   c. Providing a monthly reconciliation of all TTUHSC El Paso 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. Providing Information Technology (IT) with a master list of merchants IDs for use in overseeing technology security as it pertains to PCI DDS compliance and related storage of data on secure servers. Additionally, as liaison between the Credit Card Processor and the TTUHSCEP departments including IT, Accounting Services will notify IT of any correspondence from Credit Card Processor regarding PCI-DSS standards and/or related information requests.

6. Information Technology (IT) is responsible for establishing policies and procedures to ensure technology security as it pertains to processing of credit cards, including but not limited to PCI DDS compliance and storage of sensitive date on secure servers. Please refer to Information Technology policies at http://www.ttuhsc.edu/hsc/op/op56/.

7. Each Department/Clinic is responsible for the following:

a. Continued compliance with this OP, PCI-DSS, and TTUHSC El Paso IT security and confidentiality policies.

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

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

c. 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.

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

e. 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.

f. Providing Accounting Services with information regarding how third party processor transactions will be handled through TTUHSC El Paso 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.

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

h. 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.

i. 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.

j. 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 El Paso 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.

k. Maintaining a record retention and disposal policy to keep information storage to a minimum.

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

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

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

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

8. **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. The HSC El Paso accountant responsible for credit card processing can be contacted at (915) 215-4790.

c. Information Technology can be contacted for information pertaining to eCommerce or issues with the TTU System eCommerce Payment Gateway at 915-215-4111.