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 Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to establish the standard institutional procedure for acceptance of payment cards by university departments and set the framework to comply with Payment Card Industry Data Security Standards (PCI DSS) requirements.

REVIEW: This HSCEP OP will be reviewed by July 1 of every year (EY) 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 July 31.

POLICY/PROCEDURE:

1. **Overview**

The Payments Card Industry Data Security standards (PCI – DSS) are a set of requirements intended to ensure that all entities that process, store, or transmit credit card information maintain a secure environment. These requirements set the framework for a complete payment card data security system and process that encompasses prevention, detection and appropriate reaction to security incidents. TTUHSC El Paso must comply with these requirements regardless of the processing method.

2. **Approved Methods of Processing Payment Cards**

a. Point of sale terminal.

b. E-Commerce applications (online/web based).

c. PCI-DSS compliant third-party solutions for processing e-Commerce transactions (With approved exception request only – see paragraph 3.c below).

3. **Establishing Payment Card Services**

a. Point of sale terminal processing

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 Accounting Services at accountingelp@ttuhsc.edu. Accounting Services will obtain all necessary ID numbers, set up accounts with the credit card processor, and order credit card terminals for those merchant IDs established through the payment card processor covered under the system wide credit card agreement. 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.

b. E-Commerce applications (online/web based)

All e-Commerce applications must utilize the Texas Tech University System e-Commerce Payment processing solution (TouchNet) unless otherwise approved (see PCI-DSS compliant third-party solutions below for more information). An e-Commerce Service Request Form must be submitted for all e-Commerce applications. The request can be accessed at https://elpaso.ttuhsc.edu/fiscal/businessaffairs/accounting/forms.aspx. 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. 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 and Institutional Security Officer.

c. PCI-DSS Compliant Third-Party Solutions (for processing e-Commerce Transactions)

In some cases, consideration may be given to the use of a PCI-DSS compliant third-party solution for processing e-Commerce transactions, which are not processed through the payment card processor covered under the system wide credit card agreement. An e-Commerce Service Exception Request Form 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 and Institutional Security Officer. The e-Commerce Service Exception Request Form can be accessed at https://elpaso.ttuhsc.edu/fiscal/businessaffairs/accounting/forms.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 and providing the merchant IDs as needed by Institutional Offices including Accounting Services, Information Technology, Compliance, and Audit.

4. **Payment Card Processing and PCI Compliance Responsibilities**

a. **Accounting Services**

i. Request, provide, and maintain a master list of merchant IDs that have been established through the payment card processor covered under the system wide credit card agreement.
ii. Maintain a master list of credit card handlers.
iii. Provide a monthly reconciliation of all TTUHSC El Paso bank accounts that receive deposits, adjustments, and fees related to payment cards.
iv. Make any necessary accounting entries related to payment card disputes and discount fees that are assessed.
v. Resolve discrepancies related to payment card transactions with the credit card processor.
vi. Provide Information Technology (IT) with a master list of merchants IDs and inventory information regarding terminals for use in overseeing technology security as it pertains to PCI-DDS compliance and related storage of data on secure servers.
vii. Serve as liaison between the Credit Card Processor and the TTUHSC El Paso departments including IT and notify IT of any correspondence from Credit Card Processor regarding PCI-DSS standards and/or related information requests.

viii. Annual PCI Compliance Training

b. **Information Technology**

i. Assign Security Assessment Questionnaires (SAQs) to Merchants/Departments on an annual basis.
ii. Maintain list of all Third-Party Service Providers (TSPS) including a description for each of the services provided. Information Technology will obtain the initial Attestation of Compliance (AOC).

c. **Departments**

i. SAQ Submission.
ii. Maintain payment card device list on Inventory Management System.
iii. Maintain and safeguard 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.
iv. Periodically inspect any devices that capture payment card data via direct physical interaction to look for tampering or substitution.
v. Be aware of suspicious behavior and report tampering or substitution of payment card devices to Accounting Services.
vi. Change vendor default passwords or any other security related vendor default items.
vii. Verify that customer receipts generated for e-Commerce or other methods do not display the customer's card number.
viii. Request and maintain merchant ID numbers from external vendors for all third-party systems and/or processors not covered under the system credit card agreement.
ix. Provide 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.c 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.
x. Confirm third-party PCI-DSS compliance on an annual basis.
xi. Provide any documentation required by the credit card companies to settle any and all credit card disputes and customer charge-backs.
xii. Supply Accounting Services with any documentation related to discrepancies found during the reconciliation process and promptly notify Accounting Services of any changes to the primary contact.
xiii. Notify Accounting Services of relocation of its purchased payment card processing equipment, need to dispose of the equipment, or return to Credit Card Processor if leased. Under no circumstances should terminals be sold in surplus.
xiv. Abide by state guidelines record retention rules which state that receipts and supporting documentation should be retained for 3 years plus the current fiscal year. For medical financial records including payment or refunds, the documentation must be maintained from the date of service or until all audit questions, appeal hearings, investigations or court cases are resolved plus 10

years. Records that include the full primary account number (PAN), Full Track Data, Card Verification code, or PIN number should be redacted or encrypted prior to storage. Only the first 6 and/or last 4 digits of the PAN can be kept on-file for reimbursement reasons and proof of the card used.

xv. Ensure that hard-copy materials with cardholder data are destroyed once the record retention period has passed, as follows:
- Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
- Materials are stored in secure storage containers prior to destruction.

xvi. Electronic media with cardholder data is destroyed via one of the following:
- The electronic media is destroyed.
- The cardholder data is rendered unrecoverable so that it cannot be reconstructed.

xvii. Establish a process for verifying, at least once every three (3) months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

xviii. Ensure that information will be used for business and regulatory purposes only. Access to cardholder data (physical and electronic) should be restricted to only those with business or regulatory need.

xix. Ensure that for departments accessing cardholder data via remote-access technologies, the copying or relocation of card holder data is prohibited except for those individuals with defined, documented and authorized business need. Approval shall be given by the Institution PCI Compliance Committee.

xx. Ensure that Medical Practice Income Plan (MPIP) customer service employees processing payments over the phone utilize blackout function to prevent audio recording of payment card information if available.

xxi. Ensure PANs are not sent unprotected via end-user messaging technologies (email, chat, etc.).

xxii. Notify Accounting Services of any credit card handler employment changes in order to keep an up to date and accurate master list.

xxiii. Ensure that applicable employees have read and understood this policy and those policies referenced herein.

xxiv. Ensure that the department complies with Payment Card Industry Data Security Standards and applicable HSCEP OPs, including but not limited to:
- HSCEP OP 10.09, Records Retention
- HSCEP OP 52.09, Confidential Information
- HSCEP OP 52.10, Identity Theft Prevention, Detection and Mitigation Program
- HSCEP OP 56.01, Acceptable Use of Information Technology Resources
- HSCEP OP 56.04, Electronic Transmission of Personally Identifiable Information (PII) and Protected Health Information (PHI)
- HSCEP OP 50.37 Attachment B, PCI Responsibility Matrix

5. Policy Enforcement

a. Annually, Business Affairs will conduct audits of departments that accept, handle, store, or transmit cardholder data to validate compliance with PCI DSS. This process will involve confirming that departments have implemented the necessary controls and practices to protect payment card information.

b. The following actions may be taken if Departments, Merchants, or Users do not follow TTUHSC El Paso Policies and Procedures regarding payment processing and PCI compliance:

i. Suspension of physical and or electronic payment capability.
ii. Suspension or revocation of merchant account.

iii. Removal of technology/devices from network.

c. Should TTUHSC El Paso incur monetary fines or other incidental expenses from regulatory infractions, the University may recoup these costs from the non-compliant department.