Department Procedure: Payment Card Acceptance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Modified By Dept.** | **Date:** | **Approved By SBS:** | **Date:** |
| **1.0** |  |  |  |  |
| **2.0** |  |  |  |  |

Department Name: Merchant ID:

Contact Information:

Department PCI Contact: NetID:

Department’s Account Manager: NetID:

Department Technical Contact: NetID:

PURPOSE: The purpose of this procedure is to provide guidelines for accepting payment card transactions (e.g. Visa, MasterCard, American Express, and Discover) by all Texas State University Departments.

PROCEDURES: Payment card processing will be managed to ensure all requirements and policies for accepting and processing card payments are in accordance with the Payment Card Industry Data Security Standard (PCI DSS). A designated Department PCI Contact will be required to maintain employee access lists, the department procedures, and other applicable PCI DSS documentation. Texas State’s PCI DSS compliancy is administrated by Student Business Services (SBS), Information Security Office (ISO), Network Operations, and Core Systems. All Texas State University employees that process payment cards will follow payment card acceptance procedures as follows:

1. Employee /User Access:
   1. Hiring:
      1. All employees who will process payment cards will, upon hire:
         1. Complete training: PCI DSS Training is completed through the SAP online course. Access through Training and Development; Employee Information and Legal Issues; PCI Credit Card Compliance module.
         2. Only designated employees taking payment cards will have access to payment card data, equipment, or other devices in scope for PCI DSS. These individuals will have proper training before being given access to process payment cards.
         3. Employees with access to modify Payment Card Data Environments, such as servers, desktops with PCI software, system administration, etc., must have a background check upon hire, through Human Resources.
   2. Termination:
      1. Termination will be conducted by the hiring department and Human Resources. Once termination has been decided, the department PCI Contact will record the termination date of the employee and request removal from all PCI access, including, but not limited to the following:
         1. 3rd Party Software or Point of Sale Device
         2. TouchNet MarketPlace (uStores & uPay) or other e-Commerce Web Portal
   3. A complete, dynamic list of employees that process payment cards will be kept by the Department PCI Contact (*see Attachment A*), including hire/termination dates, training, and the employee roles and responsibilities regarding payment card processing. As changes are made, a copy is given to SBS. Employee roles and responsibilities within the department are as follows:

(Roles may include: cashier, manager, supervisor, accountant, etc. Lines may be added to the table as needed.)

|  |  |
| --- | --- |
| Roles | PCI Responsibilities |
|  |  |
|  |  |
|  |  |

1. Security:
   1. All new merchant accounts and changes to processing methods will be approved by Student Business Services and the Information Security Office.
   2. All users will comply with the following security guidelines:
      1. PCI Devices will be kept in areas that are not easily accessible to the public.
      2. Applicable passwords will be maintained in accordance with the TXST password guidelines by using a word or phrase that is at least 8 characters, and contains both up and lower case letters, numbers, and special characters.
      3. Passwords should not be stored in either paper or electronic form, unless an approved password application is used. (i.e. KeePass, Password Safe, LastPass)
      4. All default passwords on PCI Devices will be changed upon implementation.
      5. Passwords will be changed every 90 days, and conform to TXST password policy [(UPPS No. 04.01.01)](http://policies.txstate.edu/university-policies/04-01-01.html).
      6. An inventory log of all PCI devices will be maintained by the PCI Contact, to include serial number, location of device, and applicable IP addresses, and other identifiers.
         1. Inventory log will be updated when adding, relocating, and decommissioning inventory.
         2. Inventory is will be reported to Student Business Services annually. *See VIII.*
      7. PCI Devices are regularly inspected for skimming devices and/or other physical tampering.
   3. Computer Access  (check if applicable):
      1. Each person with access to computers used for payment card processing will have their own unique ID and password. Sharing passwords is expressly forbidden.
      2. Access to vendor software or hosted services will be restricted to a designated single use computer. Email, internet browsing, and other office functions are prohibited.
      3. An asset inventory of all PCI devices and ancillary devices on the network will be kept and maintained by the department including network diagrams.
         1. Any changes to the PCI environment, including new or decommissioned devices will be updated immediately on the asset inventory and network diagrams.
   4. Other PCI Devices (check all that apply):

Stand Alone Terminal (dial-up or wireless):

* + 1. A monthly inspection of the terminal will be completed and logged to identify any physical tampering of the device including the swiping mechanism and/or EMV slot. *See Attachment B*.
    2. Replacement terminals will be requested through Student Business Services.
    3. Reprogramming terminals will be requested through Student Business Services.
    4. Refund and Settlement passwords are excluded from the 90-day change requirement list above.

End to End (E2EE) or Point to Point Encrypted (P2PE) Devices:

1. All encrypted devices will be approved and tested by TXST.
2. PCI certified Point to Point Encrypted devices must be inventoried using the P2PE solution provider’s inventory portal.
3. A monthly inspection of the swipe and/or EMV slot will be completed and logged to identify any physical tampering of the device. *See Attachment B.*
4. New or replacement encrypted devices will be requested through Student Business Services or through the applicable 3rd Party vendor.
   1. Other Point of Sale (POS) Devices:
5. Register systems integrated with approved PCI DSS Compliant 3rd Party Vendor Payment Applications or Service Providers.
   * + 1. Each person with access to POS devices used for payment card processing will have their own unique ID and password. Sharing passwords is expressly forbidden.
6. A monthly inspection of the swiping mechanism and/or EMV slot will be completed and logged to identify any physical tampering of the device. *See Attachment B.*
   1. Incident Management and Response:
      1. Suspected or verified PCI violations will be responded to using the Texas State University [Security Incident Management and Response guidelines](http://security.vpit.txstate.edu/services/incident_management.html).
      2. The department will annually review the University Department Incident Response Plan Procedure.
   2. Training:
      1. Annual Training will be completed, via the SAP online module, by each employee that handles payment card data, and employees that supervise those who handle payment card data.
      2. PCI Contacts will annually review this procedure and acknowledge the review, and any changes made to the procedure, by signing and dating the newly reviewed version in the table at the head of this document.
      3. PCI Contacts will disseminate training data sent by SBS outside of regular training channels.
7. Payment Card Data Handling (check all that apply):
   1. Department receives payments in the following manner:

In Person – swiped

Mail

E-Commerce Application – Marketplace or approved E-Commerce 3rd Party Vendor.

Fax (fax is maintained in a secure area, with limited access). Receiving payment card data via fax is discouraged. Fax machines are analog phone line only, and not connected to the network.

Phone

* + - 1. The phone system is called
      2. The phone system is Voice Over IP  Yes  No
      3. The phone calls are recorded  Yes  No

Self-service Payment Kiosks, provided by department.

* 1. Payment Card Data is never accepted via email. If payment card data is erroneously received, the email will be deleted immediately from the email box and the deleted folder by pressing Shift + Delete.
  2. All payment cards are processed immediately, or within one business day.
  3. The 3-digit security code on the back of the card and the expiration date is never stored on paper or electronically.
  4. The last four digits of the payment card number may be retained.
  5. Truncated payment card receipts and settlement reports are sent to SBS for reconciliation and storage.
  6. All paper forms used to collect payment card data are formatted so the data can be easily redacted or removed for cross-cut shredding.
  7. Redacting payment card data is completed in the following manner:
     1. The payment card number is removed from the paper form, if applicable, and is immediately cross-cut shredded, ***or***
     2. The payment card data is blacked out as thoroughly as possible. The paper form is then copied and the copy is stored. The original form is immediately cross-cut shredded.
     3. Forms that are appropriately redacted or truncated may be retained for the length of time deemed necessary by the department.
  8. All payment cards are settled daily for deposit.
  9. E-Commerce transactions are cardholder initiated transactions. Employees will not process transactions through their E-Commerce application on behalf of the cardholder. Employees will not direct cardholders to use University computers to initiate e-commerce transaction, unless the computer is designated as a payment kiosk.
  10. Payment Card Data Storage:
      1. Payment Card Data is only stored temporarily, not to exceed 1 business day, in order for authorization and settlement to occur.
      2. Payment Card Data is only stored in a secured, locked area, with limited access, prior to authorization. Payment Card data is never stored in paper form following authorization.
      3. Un-redacted payment card data is never sent to SBS Cashiers Office or other records storage facilities.
      4. Departments that must store receipts or forms with redacted cardholder data, may do so only with SBS approval.
      5. All payment card receipts will be kept for only 1 year, unless otherwise specified by law for longer storage. (i.e. grants, donations, research, etc.)
      6. Payment Card Data cannot be stored on the following devices:
         1. Computers, personal or University owned (i.e. email, spreadsheets)
         2. Application or program that runs on a desktop workstation
         3. Jump or Flash Drives
         4. Non-PCI approved Devices
         5. A rolodex or other type of manual system

1. Payment Card Processing (check all that apply):
   1. Card Not Present Transactions – only with pre-approval from SBS.
      1. When applicable, keep your computer, or card processing device out of the line of sight of others.
      2. Payment card information should only be written down if card data cannot be entered directly in the computer or other card processing device, or card information was received on a form or through the mail.
         1. After the transaction is authorized, all but the last four digits of the payment card number should be redacted appropriately (*see III.H*), or removed from the form and cross-cut shredded.
         2. Written payment card data must be authorized immediately, or within one business day of receipt. Any payment card numbers that are kept overnight will be locked in a secure area with limited, need to know access.
      3. The cardholder’s billing zip code should be entered for address verification.
      4. If the card is declined, the card may be run one more time to verify the decline was not caused by data entry.
      5. Employees will not ask for payment card information to be emailed or faxed.
         1. If faxed payment card information is received, redact or cross-cut shred after the transaction has been authorized.
         2. If emailed payment card information is received, promptly delete the email from your in-box and deleted folder after the payment card number has been authorized.
   2. Card Present Transactions:
      1. When applicable, keep your computer, or other card processing device out of the line of sight of others.
      2. Swiping the card is the most secure method of accepting payment cards. Keep the card while it is authorizing and the customer signs the receipt.
      3. Compare the receipt signature to the signature on the credit card to make sure they match. If they do not match, ask for a secondary form of identification.
      4. If the card is declined, the transaction must not be run again. Ask for another form of payment.
      5. If an EMV (aka Chip and PIN) card is presented and the PCI device is enabled for this processing method, the card will be processed as an EMV card.
   3. Refunds:
      1. Refunds must be issued using the same mode of processing that was used for the original transaction.
      2. Refunds must be issued to the same payment card number that was used for the original transaction.
      3. If the card holder can provide documentation that the original payment card account number has been closed, the department may issue a refund via a Payment Request through Accounts Payable.
      4. The refund amount may only be up to the amount of the original transaction.
      5. Refunds must be approved by a supervisor, for dual control, by the supervisor signing the refund receipt attached to the original transaction receipt.
   4. Cardholder Disputes:

*Cardholders may dispute their charges through their card issuing banks and request either a copy of the receipt or transaction data, or request a full refund as a chargeback. Disputes are managed by SBS, and SBS will respond to all disputes within the allotted time frame.*

* + 1. Departments will supply requests for information regarding a dispute within 2 business days. Failure to respond to SBS with the requested information, within 2 business days, may result in a permanent loss of revenue for the disputed transaction.

1. Change Management  (check if applicable):

*Modes of processing that require Change Management are: 3rd Party Software hosted on Campus, Virtual Terminals, Kiosks,*

*Re-Directed Software or applications, and IP Terminals.*

* 1. All changes and updates to the operating system, hardware, IP, or software of a PCI system are categorized as one of the following. The [UIT procedures](http://fbs.admin.utah.edu/download/ecommerce/Roles_Procedures_Change_Management_2012_v3.pdf) will be followed for each change.
     1. *Standard Change:* Well documented, low risk, and proven. Standard changes are done on a regular basis and been implemented successfully multiple times before. The first instance of a standard change needs to be reviewed before implementation. Afterwards, standard changes are considered pre-approved and can be implemented during the next available change window without approval or using required lead times. Coordination activities can be done at the discretion of the Technical Support Person (TSP).
     2. *Minor Change:* A minor change has a low impact either in terms of the number of users affected or the criticality of the service and has a low risk of failure. Minor changes are reviewed by the Change Management team and approved by the Change Manager. Minor changes need to have the required lead time. Coordination activities can be done at the discretion of the TSP.
     3. *Major Change:* A major change has significant impact on users or services, a high risk of failure, or is complex and requires multiple teams to implement. This may also include new, high-profile applications that are being used in production for the first time or changes to applications where a high degree of coordination between multiple organizations needs to occur.
     4. *Emergency Change:*  This is a change that needs to be implemented IMMEDIATELY to fix an incident due to severe loss in service capability.
     5. *Significant Change:* May include standard, minor, major or emergency changes. **From PCI Guidance:** The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Refer to [Significant Change Requirements.](http://fbs.admin.utah.edu/download/ecommerce/Significant_Change.pdf)
  2. All changes are requested through and documented in the Information Security Office Change Management System.
  3. Department change management logs will be given to ISO and SBS upon request.

1. Vulnerability Scans  (check if applicable):
   1. Internal PCI Vulnerability Scans are run on a monthly basis by the Information Security Office.
   2. External Scans are conducted for all public facing systems. (check if applicable):
      1. External Scans will be completed at the beginning of each month.
      2. The external scans will be repeated weekly until the scan is passing and can be attested by our Approved Scanning Vendor (ASV).
   3. All vulnerabilities will be addressed within a maximum of 30 days of the finding.
      1. False Positive vulnerabilities will be documented as such.
      2. True vulnerabilities will be remediated as soon as possible, and no later than 30 days of the finding.
   4. Any changes to IP addresses, additions, and deletions will be documented through a request for change, and the Information Security Office will be notified to make the changes for the vulnerability scans.
2. Penetration Testing  (check if applicable):

*Modes of processing that require Penetration Testing are: 3rd Party Software hosted on Campus and Re-Directed Software or applications. Others modes will be tested as deemed necessary by a Qualified Security Assessor.*

* 1. A Penetration Test will be completed by qualified personnel, internal or externally contracted, on the applicable PCI systems at least once a year.
  2. Any significant changes to the PCI System, as defined in V.A.5, must be followed by a penetration test, to be initiated within 30 days of the significant change.
  3. Any findings that may pose a risk of breach to the system, or do not meet standard best practices, will be remediated within 30 days of the finding. Testing of the remediation will follow.

1. Asset Inventory
   1. A complete inventory of PCI devices and components must be kept current by the PCI Contact.
   2. Any changes made to the PCI devices inventory will be updated immediately and a copy sent to Income Accounting and Student Loan Services.
   3. A monthly inspection of all swipe and EMV capable devices will be completed and logged. See Attachment B.
   4. The asset inventory includes, but is not limited to the following:
      1. Serial Number of each PCI device
      2. Make and Model of each PCI device
      3. Location of each PCI device
      4. Purpose of each PCI device
      5. IP addresses
      6. VLANs
      7. MAC address
      8. Firewalls
   5. Asset Inventory for Stand Alone Terminals, IP Terminals, and E2EE devices:

(Lines may be added to the table as needed.)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Serial Number  (i.e. 7315197CT010246) | Tamper Tape # | Make/ Model  (i.e. iCT250 or Vx680) | Location  (i.e. front desk) | IP Address  (IP terminals only) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Addendums  (check if applicable):
   1. Addendums have been added for specific PCI procedures for the department not listed in this procedure.
2. Attachments (check all as applicable):
   1. Employee List
   2. Monthly PCI Device Inspection Log
   3. Department Form(s) for payment card collection
   4. Asset Inventory for PCI Cardholder Data Environment
   5. Updated Network Diagram
   6. Change Management Log