CUSTOMER

Departmental Payment Card Policy and Procedures

Department Name:
Business Process Owner/Title:
Last Reviewed:

Purpose

The purpose of this policy is to establish business processes and procedures for accepting and handling payment cards at **CUSTOMER** as established by the Payment Card Industry Data Security Standards (PCI DSS) and in accordance with the **NAME OF POLICY.** In order to maintain compliance with PCI DSS, it is essential that departments that store, process, or transmit cardholder data adhere to procedures within the university and departmental policies to help ensure the safe handling of cardholder data.

Collection and processing of card payments, will be conducted in compliance with standards established by the Payment Card Industry Security Standards Council (PCI SSC), University policies, and the procedures outlined in this document. Departments are responsible for ensuring all processes, procedures, and technologies follow the security standards dictated by the PCI DSS and as approved by Financial Services and the PCI Team. This policy is reviewed on an annual basis to ensure operational processes are documented and known to all affected parties.

Business Process - Accepting and Handling Card Payments

User Access and Physical Security: Access to **CUSTOMER**'s cardholder system components and data is limited to only those individuals whose jobs require such access. Access to cardholder systems, including all in-scope applications and Point of Sale (POS) devices, is restricted based on job responsibilities. User access requests are submitted via helpdesk tickets. Access to **SYSTEM** is role-based and permission is granted upon successful completion of all applicable training. When a user is terminated, transferred, or the job function no longer requires **SYSTEM** access, it is the Department's responsibility to communicate such changes to Financial Services.

Devices that capture payment card data via direct physical interaction with the card should be physically secured and protected from tampering and substitution. This includes periodic inspections of Point of Sale (POS) device surface to detect tampering and training personnel to be aware of suspicious activity. User access to sensitive areas that store, process, or transmit cardholder data is restricted based on individual job function.

Annual Awareness Training: In accordance with PCI DSS Requirement 12.6.1, all users within the department authorized to handle card payments will complete the annual PCI DSS awareness training. The annual PCI DSS training is intended to promote employee awareness of technical and operational requirements to protect cardholder data. Upon hire, the department's business process owner will notify Financial Services of any new staff required to complete training.

Payment Card Terminals: Purchase or rental of payment card terminals, including mobile applications, must be coordinated through Financial Services – only devices and locations that have been approved and tracked by the PCI Team may be used in any way associated with payment card processing. All devices must meet PCI DSS standards. The department is responsible to ensure that only authorized staff have access to the terminal and are properly trained. Terminals must be inventoried with Financial Services and must be maintained in a

secure location. Sharing or transfer of wireless terminals between departments is not allowed without proper approval from Financial Services. It is the department's responsibility to coordinate efforts with Financial Services to ensure that terminals are updated with the most recent software version to reduce processing errors.

Departments may use rented wireless terminals on a temporary basis to accept in-person card payments at specified times as agreed upon on the rental agreement. Rented terminals are kept in a secured location/locked when not in use. Use of rented terminals follows the same processing procedures for in-person payments as outlined within this document. Rented terminals are checked for tampering and the Terminal Security Sheet is completed.

Batch Settlement: Terminals must be settled no less frequently than daily. It may be prudent, given the level of activity, to settle batches on a more frequent basis. The department must maintain (for seven years) all signed receipts and card swipe terminal Batch Total Settlement Reports.

SYSTEM settles each night automatically. At 12:00 EST, a batch for each merchant is closed for the day's activity and sent to the credit card processor. Funds are posted to **ERP** based on the departments' merchant account ID and ID provided to Financial Services. Departments will establish and maintain appropriate segregation of duties between card processing, processing of refunds, and the reconciliation of payment card transactions. Each department is responsible to reconcile sales transactions to their general ledger no less than monthly.

Disputes and Chargeback: Financial Services will receive and report chargebacks and transaction disputes to the department. Departments can either accept or reject the chargeback. If rejected, the department will provide supporting documentation to justify that the transaction is valid. Failure to respond within the allocated timeframe will result in a loss to the department. Prompt attention to these matters is a priority. It is the department's responsibility to develop appropriate internal controls to mitigate risks related to chargebacks.

Equipment & Use Overview:

Physical Equipment:

Equipment Type	Equipment Name	Terminal ID	Serial Number	Location/Physical Security	Purpose of Use

Card not present usage:

For credit card merchant ending:

Purpose of use:

Physical Security Procedures:

1. Upon hire, staff are trained to be in compliance with standards established by the PCI SSC, **CUSTOMER** policies, and the operational procedures outlined in this document. In addition, staff are also trained to be aware of methods in which devices can be tampered with or replaced. Training includes the following:
    a. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
    b. Be aware of suspicious behavior. For example, attempts by unknown persons to unplug or open devices.

c. Do not alter or attempt to troubleshoot terminals. Troubleshooting support is provided by Financial Services.

2. At the start of each day (prior to use), the terminal surfaces are checked to detect tampering or substitution. Using the Terminal Security Review Sheet <insert location where the sheet is housed>, verify that the device has not been swapped with a fraudulent device by performing the following steps:

a. Compare the serial number and model number listed on the terminal to that included on the Terminal Security Review Sheet.
b. Review the tamper evident stickers on the surface of the terminal and make sure it is intact.
c. Inspect the terminal and review for foreign objects (i.e. skimmers), unexpected attachments or cables plugged into the device, pry marks, broken or stressed seams.
d. If you notice anything unusual or suspect that the terminal has been tampered with or substituted, contact Financial Services immediately at commerce@customer.edu.
e. When mobile terminals are changing hands between department users, an additional tamper check will be performed by the responsible party upon return.

Payment Card Processing Procedures:

1) **Mail Order – The department receives mail orders for xxx and credit card information is returned on the form.**
   a) Process mail orders via swipe terminal
   b) Shred mailed in form containing CHD with a cross-cut or micro-cut shredder

2) **Fax Order – The department receives orders via fax at xxx-xxx-xxxx which is located xxxx. This fax machine is secured (how).**
   a) Process faxed order via swipe terminal
   b) Shred faxed order in form containing CHD with cross cut shredder

3) **Phone Order – The department will accept credit card orders via phone only to XXX (number) and XXX (position).**
   a) Credit card information will be taken and entered directly into credit card swipe terminal. No numbers or information will be written down.
   b) Confirmation Number will be given to customer once card is accepted.

4) **Email Order - N/A – CUSTOMER does not accept credit card numbers sent in via email.**
   a) The credit card payment will NOT be processed.
   b) If numbers are received via email a response will be sent to the customer. The response will be a separate email – not a response to the original email, indicating the policy and procedure for sending credit card information.
   c) The email will be permanently deleted from email in box and trash.

5) **In Person – The department accepts credit card payment in person at xxx office.**
   a) Request card from cardholder for processing. Ensure card is signed, if not, request ID.
   b) Process transaction via swipe terminal.
   c) Have customer sign merchant copy/receipt. Verify signature matches back of card. Ask for photo ID from any customer without a signature on back of card.
   d) Give card and receipt to customer.

6) **On-line Orders**
   a) Online orders are taken via the Department's online solution **SYSTEM** at xxx (link).

b) Department individuals with authorized access to **SYSTEM** will fulfill orders on a daily basis.

Refund Procedures: Clear disclosure of return, refund, and cancellation policies can help to prevent potential cardholder disputes/chargebacks. Visa/MasterCard will support refund policies provided they are clearly disclosed to cardholders. Departments using **SYSTEM** must communicate refund/return/cancellation policy either in the sequence of pages before final checkout with a click to accept button or checkbox on the checkout screen / location with electronic signature.

1. The department's refund policy is **xxxxxx**
2. Procedures to refund a credit card transaction are included in the user manual for the POS devices and **SYSTEM**.

Incident Response Procedures: An incident is defined as a suspected or confirmed data compromise in which there is a potential to impact the confidentiality or integrity of payment card data. A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted payment card data is collected, processed, stored, or transmitted. In the event of a suspected or confirmed incident:

1. Call the **CUSTOMER** Help Desk at **xxx-xxx-xxxx**.
2. Unplug the network cable.
3. Do not access or alter compromised systems.
4. Do not turn off the compromised machine.
5. Refer to Incident Response Plan for further instructions.