DEPARTMENT NAME Payment Card Procedures

Any department accepting payment cards on behalf of the University for goods or services should designate a full time employee within that department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. This individual will be responsible for the department complying with the security measures established by the payment card industry and university policies. In addition, they are responsible to ensure any employee who processes transactions takes the employee PCI training/acknowledgement and, if applicable, have the appropriate background check completed before any access is granted to the employee.

Departments may only use the services of vendors which have been approved by Bursar's Office to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order or internet based.

Each Department that Handles Credit and/or Debit Card Information Must Have Documented Procedures for Complying with this Policy and PCI-DSS.

Each department that handles credit and debit card information must have written procedures tailored to its specific organization and are consistent with this policy and PCI-DSS. Departmental procedures should be reviewed, signed and dated by the Department Manager on an annual basis indicating compliance with the University's Credit and Debit Card Policy.

Departmental procedures must thoroughly describe the entire transaction process and will include, but are not limited to, the following:

- Segregation of duties
- Deposits
- Reconciliation procedures
- Physical security
- Disposal
- Cash register procedures (if applicable)

Note - For assistance in developing departmental procedures, contact the University Credit Card Coordinator.

General Payment Card Procedures

Do...

- Verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements.
- Verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS).
- Ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable.

Do not...

- Store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card, after authorization.
- Have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked.
- Store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones.
- Permit any unauthorized people to access stored cardholder data.

Payment Card Procedures – In-Person/Mail Order/Telephone/Faxed orders – swipe or key enter into swipe terminal

Receiving" in-person" payment information from a customer: (attach copy of registration form where payment card information is requested)

- Only approved staff should be handling credit card transactions.
- Card Handling Guidelines
    - Review Card Security
        - Is the Card valid? The card may not be used after the last day of the expiration month embossed on the card.
        - Only the actual card/account holder should be using the card.
        - Does the customer's signature on the charge form match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.
        - Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.

        - Does the account number on the front of the card match the number on the back of the card and the terminal receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.
        - Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.
    - Risks of Keyed Transactions
        - Manually keying in the Card account information to get an authorization carries a higher risk of fraud since many of the built-in Card security features cannot be accessed. If the magnetic stripe on the back of the Card is unreadable, or if you choose to process transactions manually, follow these steps:
            - Key the transaction and expiration date into the terminal for Authorization approval.
            - Ask the cardholder to sign the paper receipt and compare the signature.
    - Report Suspected Card Fraud
        - If you suspect card fraud report it to your bank using their established procedures
- Retain the signed merchant copy of the swipe machine generated receipt, the cardholders copy should be returned to the cardholder.
- Registration form with some verification of type of payment and date is forwarded to individual managing the event or class, etc. (use a reference point to locate the original merchant receipt if credit is later issued)
- Place merchant copy of payment card receipt in _____ until the end of the day batch process has been run.
- Oversight of the swipe machine during business hours:
    - Log information into the Swipe Terminal Inventory Sheet and periodically check the machine (verify stickers have not been removed and re-affixed, same model, etc) to determine if it has been tampered with or exchanged. Report any tampering as a security breach, see below.
    - Keep the machine in a location not easily accessible to the public,
    - Keep the machine in a locked area when not in use or after hours,
    - Machines that are deemed NOT tamper-proof are disconnected and lock in a safe area when not in use or after hours.

Individuals responsible for handling in-person payments: _____

_____

_____

_____

Receiving payment information from a customer: (attach copy of registration form where payment card information is requested)

- Two people open mail in the AM and log (see _____ instructions)
- Form with payment card information handed over to individual responsible for key entering CC data (attach cover sheet with date, count and initials of mail clerk)
- Key enter card information as prompted,
- Obtain two copies of swipe machine generated receipt,
- The payment card information is removed and cross-cut shredded or rendered unreadable on the form (hole-punch through the card number, expiration date and security code) after the transaction has been processed,
- Registration form with some verification of type of payment and date is forwarded to individual managing the event or class, etc. (use a reference point to locate the original merchant receipt if credit is later issued)
- Place merchant copy of payment card receipt in _____ until the end of the day batch process has been run.

Individuals responsible for opening and distributing the mail: _____

_____

Individual with responsibility for Swipe transactions: _____

Backup personnel for Swipe: _____

Batching out process at end of day:

- Follow the bank's procedure to settle transactions at the end of the work day.
- Staple the settlement sheet in front of the sales receipts and

  Either, store in a secure location (safe,) until morning or,

  Or, deliver to FINANCIAL TEAM who is responsible for GL entries who locks the settlement in a secure location (safe) until morning.

Individual responsible for batching transactions: _____

Backup for batch process: _____

General Ledger (GL) process:

- Follow instructions in GL DOCUMENT/INSTRUCTIONS,

- File settlement documents in a secure location pending monthly reconciliation of the credit card clearing projects.

Fiscal person with GL responsibilities: _____

Reconciliation process:

- Follow instructions in RECONCILIATION DOCUMENT.
- Attach GL reports and settlements and file in a secure location.

Individual responsible for reports and reconciliation: _____
Approver: _____

Storage of Reconciliations and Settlement:

- Label file contents and note date to be destroyed.
- Log location and movement of files until destruction as per Records Management

Individual who tracks and maintains the log: _____

Other considerations

Security of Swipe Equipment

Oversight of the swipe machine during business hours:

- Log information into the Swipe Terminal Inventory Sheet and periodically check the machine (verify stickers have not been removed and re-affixed, same model, etc) to determine if it has been tampered with or exchanged. Report any tampering as a security breach, see below.
- Keep the machine in a location not easily accessible to the public,
- Keep the machine in a locked area when not in use or after hours,
- Machines that are deemed NOT tamper-proof (anything other than a Hypercom 4210) are disconnected and lock in a safe area when not in use or after hours.

Response to clients that send credit card information through email

Purpose: As part of the University's PCI DSS compliance program, we are enforcing a policy for all colleges and departments that perform credit card transactions. Part of that policy addresses the receipt

and sending of credit card data through any open communication systems such as email or chat programs.

Policy: Any open communication system such as email or chat programs may not be used for the receipt or transmission of any credit card information. If a client should send their credit card information to the department, the following steps should be taken:

1) Click "Reply" on the email
2) Delete the credit card number from the original portion of the email.
3) In your response, Copy and paste the following
    a. "Thank you for contacting (*insert department or name)*. We appreciate your business, however as part of our compliance effort with the Payment Card Data Security Standard and our practice to protect all of our clients Personally Identifiable Information, we cannot process the Credit card information that you have sent through email. We ask that you use one of the accepted methods of processing the sale. Those methods are:
        - Our Online form at (http:// xxxxxxxxxxx.edu)
        - Mail
        - Phone
        - Fax to:
4) Then promptly delete the original email and empty the trash.
    a. If the IT department has implemented a "SECURE DELETE" feature, use this.

Fax receipt of Payment Card information

- Fax machine is located in an area not accessible to the public,
- Documents are immediately distributed to the individual responsible for key-entering the information into a swipe terminal,
- The payment card information is removed and cross-cut shredded or rendered unreadable (hole-punch through the card number, expiration date and security code) after the transaction has been processed
- The merchant copy is attached to the fax and filed in an appropriate place
- The customer copy is faxed/mailed/emailed back to the customer (optional).

Suspected breach of security or fraud

- Notify your supervisor and your department PCI Coordinator
- Follow the UGA Computer Security Incident Policy