Departmental/Merchant Payment Card Procedures

Merchant Name _____ Merchant ID # _____

Department Merchant Liaison _____

I. Overview

These merchant procedures apply to all departmental personnel who handle cardholder data (CHD) on behalf of George Mason University whether on the University campus or at a remote location.

Any merchant accepting payment cards on behalf of the University for goods or services must designate a full time employee as the Department Merchant Liaison. This individual has primary authority and responsibility for payment card and/or ecommerce transaction activity within the department. They ensure that the department as a merchant adheres to the university Payment Card Security Policy (#2110) and related procedures and policies, and complies with the current Payment Card Industry Data Security Standard (PCI DSS). Additionally they are responsible for ensuring that all departmental staff handling payment card transactions receive annual PCI DSS training and sign an acknowledgement of the University's Payment Card Control & Security Procedures.

Each merchant must have written payment card procedures tailored to its specific organization that comply with current university policies, procedures and the PCI DSS. The Department Merchant Liaison should review the procedures annually and sign and date below acknowledging compliance with current requirements.

All payment card processes of the university, including the use of any third party vendor service, must receive advance review and approval from Fiscal Services and IT Security.

II. Procedures

Department Liaison Review:_____ Effective Date_____

General Information:

- Revenue Description (What type of revenue received / how often / from whom)
  _____
  _____
- How Payment Card Data is Received (circle all that apply) - Online / In Person / U.S. Mail / Fax / Phone
- If Online, Software and Gateway Used:_____
- Is Payment Card Authorization Form Used? Yes / No (circle) [if yes, attach a copy of the form]

Segregation of duties:

- General Limitations and Obligations:
  - One person cannot have exclusive access to all roles(biller/collector/depositor/reconciler)
  - The person collecting and/or depositing cannot also be the biller or reconciler.
  - A backup must be designated for each role in the event of unexpected absence.

- Designations (List position titles. List N/A if role doesn't apply to your department's process):
  Biller: Primary_____ / Backup_____
  Collector: Primary _____ / Backup_____
  Depositor: Primary _____ / Backup_____
  Reconciler: Primary _____ / Backup_____

Functions & Steps (For each function list primary steps, include who, how, when & frequency or enter N/A if function not applicable) :

- Billing/Invoicing :

_____

_____

_____

_____

_____

_____

- Collection of Payment Card Data (this function not applicable if collected online) :

_____

_____

_____

_____

_____

_____

- Deposit of Payment Card Data (process to settle batches & prepare/send report to Treasury Accountant) :

_____

_____

_____

_____

_____

_____

- Reconciliation (include both automated and manual steps; clearly list what is done, how often, by who & reports used):

_____

_____

_____

_____

_____

_____

Physical Security and Storage of Cardholder Data

PCI DSS Definition of Cardholder Data – At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN **plus** any of the following: cardholder name, expiration date and/or service code.

- Describe how and where Cardholder Data is secured and stored from receipt until processed:

_____

_____

_____

_____

_____

_____

- Is Cardholder Data kept after processing? Yes / No (circle)
  [If yes, indicate why it is needed, what is stored, how/ where it is secured and for how long it is kept. If no, enter N/A]

_____

_____

_____

_____

_____

_____

Disposal of Cardholder Data

- Describe in detail the specific method used to dispose of Cardholder data (i.e. "cross-cut shredder" not just "shredder") and what data is destroyed (i.e. is the entire authorization form destroyed or are only CHD items, such as the full PAN, removed and then destroyed):

  _____

  _____

  _____

General Guidelines and Considerations

In-Person Transactions:

- Review the card for validity:
    - Has the card expired? (It may not be used after the last day of the expiration month)
    - Does the customer's signature on the charge slip match the one on the back of the card?
    - Does the signature panel on the card look normal? (assuring it has not been physically altered)
    - Does the account number on the card match the number on the terminal receipt display?
    - Does the name on the customer receipt match the embossed name on the card?
- Retain the signed merchant copy of the receipt, give the customer copy to the cardholder. Each receipt should contain only the truncated or masked card number (e.g. last four digits).
- Manually keying in the CHD to get an authorization carries a higher risk of fraud since many of the built-in security features cannot be accessed. This should only be done if the magnetic stripe on the back of the card is unreadable.

U.S. Mail, Fax or Phone Transactions (CHD via phone or authorization form & keyed into dialup POS terminal):

- Only authorized and trained personnel should handle payment card transactions.
- For Mail receipt – Mail is opened and the payment logged, preferably in the presence of another person.
- For Fax receipt – Must be via a non-networked machine located in a secure area.
- CHD should be promptly keyed on a dialup POS terminal (or securely stored until entry)
- Receipts should be printed with the card number truncated; retain one and send one to customer.
- CHD should be properly destroyed immediately after processing (use cross cut shredder or hole punch).

E-Commerce Transactions:

- Customers should enter their own transactions on the device of their choice. Departments may not direct the customer to a specific computer or location to pay.
- GMU computers should never be used by GMU employees for payment card entry on behalf of a customer.
- Settlement reports / transaction receipts should include only truncated card numbers.

Other Considerations:

Security of Swipe Terminals (card reading devices used in card-present transactions)**:**

- Each department must maintain a list of all card-reading devices they own/use.
- This list must be kept current and include the make, model, serial # and physical location of each device.
- Periodically inspect the serial number, surface and condition of each device to look for signs of tampering or substitution. Log inspection data into the Swipe Terminal Inspection Sheet (copy attached).
- Ensure all POS staff are trained to be aware of suspicious behavior and know how to identify and report any attempted tampering or replacement of devices.
- During operating hours, keep all devices in a location not easily accessible to the public.
- When not in use or after hours, lock or secure the area where devices are located.

Suspected breach of security or fraud:

- Notify your supervisor and Fiscal Services Internal Control at **(703) 993-7010 or (703) 993-2466.**

- If the suspected activity involves computers (hacking, unauthorized access, etc.) report actual or suspected electronic security incidents to IT Security at **(703) 993-4183 or (703) 993-4557**. Cease use of the computer immediately, understanding that continued use may inadvertently damage potential evidence in the event that the electronic security incident becomes part of a criminal case.
- If you are unsure but suspect fraud, you should contact the University Police at **(703) 993-2810.**

Response when CHD is emailed:

- As part of the University's PCI DSS compliance program, the receipt and sending of payment card data through any open communication systems such as email or chat programs is strictly prohibited. These are not secure methods to transfer CHD. You should not advertise that email is acceptable and you should never accept or process a payment card number that comes to you unsolicited. You should also never email CHD to another department. If you receive unsolicited CHD in an email or an email attachment, the following steps should be taken:
    1) Do not process it.
    2) Notify the sender that the payment has not been processed. Do not reply to their original email unless you have first deleted the payment card number or, you can notify them via a new email.
    3) Give alternatives, let them know the acceptable ways to transmit CHD.
    4) Promptly delete their original email and, then empty it from your Deleted Items folder.

Use of third party service providers (to collect, transmit, process or store CHD)**:**

- Each department must maintain a list of all service providers with whom cardholder data is shared, or that could affect the security of cardholder data.
- Prior to engaging a service provider, the department must have Fiscal Services and IT Security approval.
- A written agreement must exist that includes an acknowledgment that the service provider is responsible for the security of CHD they possess or otherwise store, process or transmit on behalf of the customer to the extent that they could impact the security of the university's cardholder data environment.
- Each provider's PCI DSS compliance status must be monitored at least annually.
- Information must be kept regarding which PCI DSS requirements are managed by each service provider and which are managed by Mason.