



ADMINISTRATIVE PROCEDURES

TITLE: Merchant Cards		PROCEDURE #: 493-A
DEPT: Treasurer's Office		DIVISION: NA
EFFECTIVE DATE: 5/13	REVIEWED:	REVISED:

OBJECTIVE: To establish a procedure for receiving and processing merchant card transactions.

REFERENCE: Policy #493

POLICY STATEMENT: Ensure county employees protect cardholder information against theft and/or improper usage, comply with all credit and banking industry security regulations related to payment card processing and reporting, and maintain proper financial controls in the receipt and processing of payment card transactions.

APPLICABILITY: Elected officials, department heads, managers, supervisors, and employees who process, transmit, handle or store cardholder payment information in any physical or electronic format.

PROCEDURES:

1. Responsibilities:
 - 1.1. The County Treasurer or designee will be the PCI Compliance Manager for the county. The PCI Compliance Manager is responsible to:
 - 1.1.1. Provide training and education on merchant card processing and card data security.
 - 1.1.2. Develop, implement and update Marion County's merchant card policy and procedures as needed.
 - 1.1.3. Approve all merchant account applications to provide merchant card services to the public.
 - 1.1.4. Enroll new merchants and consult with existing merchants.
 - 1.1.5. Coordinate with merchants and the county Information Technology Department to work through technical requirements that may exist for the secure processing of merchant cards.
 - 1.1.6. Coordinate the county's merchant card processor contract and work with the county's card processor to obtain merchant identification numbers.
 - 1.1.7. Manage the county's Payment Card Industry Data Security Standard compliance activities.
 - 1.1.8. Obtain and retain a signed Merchant Card Compliance Statement from all employees handling cardholder data. This statement includes acknowledgement by the employee that he/she has read and understood the Merchant Card policy and procedures.
 - 1.2. Departments accepting merchant cards are considered Merchants for this policy. Merchants are responsible to:

SUBJECT: Merchant Cards

SUBJECT: Merchant Cards

- 1.2.1. Make application to the PCI Compliance Manager to accept merchant cards for goods and services provided.
- 1.2.2. Pay all bank fees associated with their merchant transactions.
- 1.2.3. Pay for costs of ordering and maintaining the equipment and supplies.
- 1.2.4. Follow this policy and all PCI compliance standards.
- 1.2.5. Send all employees who process merchant card transactions to Payment Card Processing training annually.
- 1.2.6. Merchants must ensure that all employees that may process, transmit, store, Reconcile, or otherwise handle payment cards sign the Payment Card Merchant Compliance Statement
- 1.2.7. Notify the PCI Compliance Manager of new employees that handle cardholder information, and ensure each new employee completes the Merchant Card Compliance Statement.
- 1.2.8. If accepting cardholder data via a fax, locate fax machine in a secure area with limited access.
- 1.2.9. Utilize only those merchant card processors and acquirers approved by the Treasurer.
- 1.3. Employees whose duties require handling of cardholder data should adhere to the following guidelines for the acceptance, processing, retention and disposal of this information:
 - 1.3.1. Verify signature of cardholder at the time of the transaction.
 - 1.3.2.. Obtain the signature of the cardholder on the receipt and provide a duplicate copy to the cardholder.
 - 1.3.3. Verify that the merchant card's expiration date is valid.
 - 1.3.4. Do not accept cardholder data via end-user messaging technologies (e.g. e-mail, voicemail, instant messaging, and text messaging).

Modifications to these guidelines may be appropriate depending on the occurrence and volume of transactions that a merchant processes.

- 1.4. Information Technology is responsible to:
 - 1.4.1. Approve and/or implement all computer networking, computer programming, and information system services necessary for the departments to provide merchant card services to the public.
 - 1.4.2. Work with the PCI Compliance Manager to meet Payment Card Industry Data Security Standard requirements related to information systems and provide documentation to the PCI Compliance Manager as necessary.
2. Application Process: In order to ensure that Marion County complies with the Payment Card Industry Data Security Standard (PCI-DSS) for merchant card security;
 - 2.1. Departments **may not** establish their own banking relationship to process merchant cards. The Treasurer's Department negotiates on behalf of all county departments, taking advantage of volume discounts not available to individual departments. Under no circumstances may a department contact a merchant card processor to obtain access to payment card privileges.
 - 2.2. The following steps must be followed for any department wanting to accept merchant cards:

SUBJECT: Merchant Cards

- 2.2.1. Complete and submit the Marion County Application for Merchant Account (Attachment A) to the Treasurer's Office.
- 2.2.2. The County Treasurer will approve applications based on the department's ability to comply with this policy and the payment card industry compliance requirements.
- 2.2.3. Once approved, the Treasurer will work with the merchant card provider and obtain the necessary hardware or software and the Merchant Account to properly configure the system to accept merchant cards.
- 2.2.4. Departments must arrange for all employees processing merchant cards to complete a Merchant Payment Processing training course offered by the Treasurer's Office prior to processing merchant card transactions. This course must be repeated and confirmed annually.
- 2.3. Prohibited activities include:
 - 2.3.1. Cash advances
 - 2.3.2. Amounts over a sale amount (cash back options)
 - 2.3.3. Adjustment of the price of goods or services based upon method of payment
 - 2.3.4. Convenience fees in card-present transactions (except where authorized)
 - 2.3.5. Providing discounts to a customer for paying with cash

3. Fees:

Each merchant card transaction is assessed a variety of fees. These fees accumulate for each merchant ID and are charged back to the responsible department on a monthly basis by the Treasurer's Office. The three types of fees assessed include:

- 3.1. The interchange fee is paid to our customer's bank and will vary by bank. This fee is not negotiable.
- 3.2. The bankcard fee is assessed by Visa or MasterCard and will vary based on the type of merchant card used (debit vs. credit), the amount of the transaction, the amount of time between authorization and settlement, and the overall perceived risk of the transaction.
- 3.3. The discount fee is charged by Marion County's merchant card processor. This fee is negotiated during an RFP process through the Treasurer's Office.

4. Payment Channels:

"Card Present" and "Card Not Present" are the two types of payment channels available. The main difference is determined by whether or not the bank-issued merchant card is available to have its magnetic track read at the time of purchase.

- 4.1. Card Present processing is used for face-to-face transactions. The customer presents his/her merchant card for payment, the card is swiped through a reader, and the customer either signs a receipt for the merchant's records or enters a PIN (Personal Identification Number). Card Present transactions are most often handled by a payment terminal or a Point-Of-Sale system.
- 4.2. Card Not Present processing is used for telephone and internet transactions. The payment card is not available to the merchant for swiping through a card reader, so the payment information must be manually keyed into the processing system. Processing merchant cards in this manner present higher fees and risks compared to processing traditional Card Present payments. These risks must be

SUBJECT: Merchant Cards

carefully analyzed to minimize any potential for a security breach and potential loss or misuse of cardholder information. Any breach could result not only in significant monetary fines to the county, but loss of the ability for the county to accept payment cards.

5. Reconciliation:

- 5.1. Departments will perform a transaction settlement procedure (close) at the end of each business day. This process electronically sends a payment file to the bank for all transactions received since the previous settlement procedure. A batch settlement report must be produced at this time.
- 5.2. The batch settlement report is attached to the individual sales receipts and filed.
- 5.3. A Treasury Merchant Deposit Spreadsheet must be created and emailed to the Treasurer's Office in the required format for every batch that is settled. This spreadsheet must be separate from the cash and check deposit spreadsheet. Frequent failure to send a Merchant Spreadsheet to the Treasurer's office that reconciles to the batch report may result in a department's loss of payment card processing privileges.
- 5.4. Treasurer's Office will match the Merchant Spreadsheet with the bank report and send a receipt back to the department.

6. Internal Controls:

Departments will develop and maintain operational procedures for each merchant terminal and submit to the PCI Compliance Manager for review. These operational procedures should address the following areas:

- 6.1. Segregation of duties: To the extent possible, departments should establish segregation of duties between merchant card processing, the processing of refunds, and financial reconciliation. Departments should also require supervisory approval for any refund transactions.
- 6.2. Reconciliation procedures: All merchant card terminals and website applications should be closed out and reconciled at least once each day, and a Merchant Spreadsheet completed and emailed to the Treasurer's Office daily.
- 6.3. Physical security of cardholder information.
- 6.4. Disposal of card holder information.

7. Disputes and Chargebacks:

A chargeback occurs when a customer has a disputed merchant card transaction and the department has either not been able to supply documentation to substantiate the transaction or has not done so in a timely basis. By law, the cardholder has two years to file a dispute. Once a cardholder files a dispute, the issuing bank makes an investigation into the complaint. If the department cannot prove the transaction to be legitimate, the bank will charge back to the merchant the entire value of the transaction, along with an additional fee.

- 7.1. When a customer disputes a transaction, the merchant card processor sends a sales draft request to the Marion County Treasurer's Office.
- 7.2. The Treasurer's Office immediately forwards each request to the appropriate department for response.
- 7.3. The department will send the required documentation of the transaction to the merchant card processor within the limited time allowed by the processor.

SUBJECT: Merchant Cards

- 7.4 The department shall retain a copy of the submitted materials and document the date when the materials were submitted to the processor.
8. Retention and Disposal:

Cardholder data cannot be retained/stored electronically or in paper form. The only exceptions are for transactions by mail and events in which a card processing device is not available for immediate processing. For both exceptions, cardholder data must be received in a paper form and must be kept in a secure, locked location with limited access. Payments must be processed within two business days of receipt and the paper form containing the cardholder data must be immediately disposed of by cross-cut shredding or depositing into a locked shred bin.
9. Security/Destruction of Cardholder Information:
 - 9.1. Merchant will not store, process or transmit cardholder information on the county's network.
 - 9.2. Merchant will never transmit cardholder information; especially account numbers, by end-user messaging technologies such as email, instant messaging or chat.
 - 9.3. Merchant will not create an electronic file containing cardholder information (database, spreadsheet, word processor, image, etc.). For internet transactions, files received from the acquiring bank will not contain any cardholder information other than the name of the customer.
 - 9.4. Merchant will never store cardholder information on portable devices, including laptops, external hard drives, flash drives, etc.
 - 9.5. Merchant will never store any cardholder information, in any physical form that is not required for business operations.
 - 9.6. If cardholder information does need to be physically retained for business purposes;
 - 9.6.1. All hardcopy media containing cardholder information is to be physically secure and retained, stored, or archived only within secure Marion County office environments.
 - 9.6.2. All hardcopy media containing cardholder information must be stored in a secure and locked container (e.g. locker, cabinet, desk, safe, storage bin).
 - 9.6.3. Hardcopy material containing cardholder information must be easily distinguishable as "confidential" through labeling or other methods.
 - 9.6.4. Distribution of confidential or sensitive hardcopy material must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked.
 - 9.6.5. At no time is printed material containing cardholder information to be removed from any Marion County department or secured storage area without prior authorization from management.
 - 9.6.6. Custodians of hardcopy media containing cardholder information must perform an inventory of the media at least annually. Results of inventories shall be recorded in an inventory log.
 - 9.7. All media containing cardholder data must be destroyed after the minimum time deemed necessary for their use has passed, or when it is no longer needed for business or legal reasons.
 - 9.8. Hardcopy media must be destroyed by cross-cut shredding, incineration, or pulping so that cardholder data cannot be reconstructed.

SUBJECT: Merchant Cards

10. Security:

- 10.1. It is the responsibility of the department to follow the county's payment card policies and procedures to ensure transactions are processed safely.
- 10.2. All departments authorized to accept merchant cards must exercise reasonable care in screening transactions to reduce merchant card misuse and loss of funds.
- 10.3. Departments must establish and maintain a proper security environment to safeguard a customer's payment information at all times.
- 10.4. Departments must process merchant card transactions using approved electronic data capture machines received from the Treasurer's Office.
- 10.5. Merchant card transactions must be done in person, by telephone, by mail, or via a secure pre-approved internet application. Never send or accept payment card information via email.
- 10.6. Procedures must be created for any paper that contains sensitive card information. The procedures must include these requirements at a minimum:
 - 10.6.1. Store all materials containing cardholder account information in a restricted/secure area. In addition, these materials should be kept in a locked file cabinet, safe, or other secure storage mechanism.
 - 10.6.2. Sensitive Authentication data must never be stored subsequent to authorization.
 - 10.6.3. Limit access to sales drafts, reports, or other sources or cardholder data to employees on a need-to-know basis.
 - 10.6.4. If paper records containing payment card account numbers are stored, all but the last four digits should be redacted within 60 days, or as soon as refunds or disputes are no longer likely, but no more than 180 days.
 - 10.6.5. Printed customer receipts that are distributed outside the department must show only the last four digits of the payment card account number.
 - 10.6.6. Card information may never be stored in a customer database or electronic spreadsheet.
 - 10.6.7. Materials containing cardholder account information must be rendered unreadable prior to discarding. Shredding must be done by cross cut.
- 10.7. If at anytime a department employee experiences or discovers a breach or potential breach of any payment information or related data, that employee must report the event immediately to the PCI Compliance Manager. The PCI Compliance Manager will assess the situation and contact the appropriate merchant services partners and acquirers to begin an evaluation and determine the appropriate level of response.

ATTACHMENTS:

Attachment A: Marion County Application for Merchant Account

Attachment B: Merchant Card Compliance Statement

SUBJECT: Merchant Cards

Attachment A



Marion County Application for Merchant Account

Send or fax the following request to:

Laurie Steele, Treasurer
PO Box 14500
Salem, OR 97309
FAX: 503.373.4401
Phone: 503.584.7750

1) Requesting Department/Division: _____

2) Merchant (Department) Information

DBA Name: _____

(The DBA name is limited to 22 characters/spaces and is the name that will appear on your customer's statements. It should reflect your department in such a way that the customer will recognize the charge. (e.g., Marion County Fair; County Health Clinic)

DBA address 1: _____

DBA address 2: _____

DBA Phone #: _____

DBA Fax #: _____

Department Contact Name: _____

Email Address: _____ Phone #: _____

3) Other Merchant Information

Description of product or services offered:

SUBJECT: Merchant Cards

Estimate annual activity per year from the payment card option:

- Average Sale Amount: _____
- Total Monthly Sales: _____

Estimate percentage of use for the following processing options:

- _____ Card present – swiped (face-to-face/over-the-counter)
- _____ Card not present – phone, mail, or fax transactions

- 4) There are three types of fees that will be charged against each transaction. The interchange fee is paid to our customer’s bank. The bankcard fee goes to Visa or MasterCard. The Discount Fee is a fee our bank charges us for their work in the processing of the transactions. The fees are charged to you monthly. Please indicate the Oracle GL costing string where card processing fees and expenses will be charged:

Fund: _____
Dept: _____
Division: _____
Program: _____
Service Area: _____
Account: _____
Project: _____ (not required)

- 5) The Treasurer will order the equipment necessary for your payment card processing. The cost of one merchant terminal is approximately \$600. Special need terminals will have additional costs. The Treasurer will contact you to discuss the type of equipment that will work best for your needs. Please indicate the Oracle GL costing string where the equipment costs will be charged:

Fund: _____
Dept: _____
Division: _____
Program: _____
Service Area: _____
Account: _____
Project: _____ (not required)

SUBJECT: Merchant Cards

- 6) Identify all employees in your department/division that may be involved in the processing, transmitting, storing, reconciling or in any other manner handling the payment cards for your division.

Each of these employees will be required to attend annual payment card training programs, as well as acknowledge that they have read, understand and will comply with Marion County's Merchant Cards policy and procedures.

Employee Name	Job Title
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

SUBJECT: Merchant Cards

After your application has been received you will be contacted to identify the most reasonable and cost effective process for your payment card processing. If a network connection or analog phone line is necessary you will be responsible for contacting the Information Technology Department for the arrangements.

You must demonstrate an ability to provide adequate controls over the processing of payments, processing of refunds, and financial reconciliation as well as adequate security procedures to protect cardholder data before your application will be approved.

I have read and agree to comply with Marion County Administrative Policy 493; Merchant Cards, and all PCI DSS requirements.

Department Contact: _____

Date: _____

Department Head Approval: _____

Date: _____

Treasurer Approval: _____

Date: _____



MARION COUNTY Merchant Card Compliance Statement

As a Marion County employee with responsibilities for handling merchant cards and/or cardholder data, I recognize that I have access to sensitive and confidential information. I will strive to protect Marion County and its customers at all times when making decision concerning payment cards and cardholder data, and I agree with the following statements:

- I have read, understand and agree to abide by Marion County’s Merchant Cards policy and procedures.
- I will utilize cardholder data for Marion County business purposes only.
- I will not use or distribute cardholder data for personal purposes. I understand that such actions are illegal and grounds for prosecution.
- I understand that in cases where I suspect a breach of security, including the suspicion that cardholder data has been exposed, lost, stolen or misused, I must immediately contact the Marion County Treasurer.
- If I am a department manager, I understand that I must maintain effective business processes for accepting, processing, retaining and disposing of cardholder data.
- I understand that failure to comply with the Marion County Merchant Cards policy and procedures carries severe consequences, which may include loss of the ability to process payment card transactions and disciplinary action, which can include termination of employment.

Employee:

Printed Name	Employee #	Date
Signature	Department/Division	

Supervisor/Manager:

Printed Name	Employee #	Date
Signature	Department/Division	