INTRODUCTION

The purpose of these procedures is to provide guidance for accepting credit card payments for services throughout Miami Dade County (County), accounting controls to mitigate risks of credit card fraud, and an understanding of the Payment Card Industry (PCI) regulations.

TABLE OF CONTENTS

I. Acceptance and Processing
   A. Handling Credit Card Information

II. Accounting Controls
   A. Chargeback Processing
   B. Refunds/Voids/Credits
   C. Reconciliation

III. Terminals

IV. Payment Card Industry Data Security Standards

V. Contract Language for Credit Card Payment Systems
   A. Vendor Form

VI. PCI Liaison

VII. Approvals

VIII. Procedures for New Credit Card Services and Equipment
   A. Template for Requesting New Services
I. Acceptance and Processing

Credit card payments shall be used for the sole purpose of processing payment transactions for services provided by the County to the cardholder. Cash advances or any cash withdrawals are not authorized to the cardholder in connection with any County card transaction.

Request for new services will be initiated through the Finance Department in accordance with section VIII of these procedures. The cost of equipment and processing credit card transactions will be paid from departmental funds. Technology implementation must be in accordance with the Payment Card Industry Data Security Standards (PCI DSS) as noted in sections IV and VIII of these procedures.

Departments must use the credit card payment processor(s) under contract with the County. The Finance Department Cash Management Division will assist departments to obtain new services and equipment working with the County’s contracted credit card payment processor. Departments shall not contact the payment processor directly for new equipment or services.

A. Handling Credit Card Information

In accordance with PCI DSS, Req. 12.6.1, all employees involved in processing credit card transactions and the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) must be trained upon hire and at least annually. The County offers an annual in-person training each January and a required on-line training course available and each department is responsible for ensuring that respective employees take the required training.

Protecting cardholder data is essential; thus, every effort shall be made NOT to store cardholder information in any form. Any physical access should be appropriately restricted to data or systems that house, process, or transmit cardholder data so as to not provide the opportunity for persons to access and/or remove devices, data, systems or hardcopies.
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

For each payment channel, the acceptable PCI-DSS compliance method is explained below:

1. **Via the phone:** Staff is prohibited from recording credit card conversation(s) and writing full credit card number(s), which should be entered directly into the system as soon as it is received from the customer. Security controls must be in place when handling payments over the phone. Ensure that conversation(s) are taken in a secured location not audible to other staff members or customers.

2. **Via U.S. Mail:** Every effort should be made not to accept credit card information via U.S. mail. If there is a legitimate business reason to accept this payment method, departments must secure the documents received. It is recommended that the mail be opened and logged in a secure room with cameras in order to restrict access to the credit card information. All credit card data must be securely cross shredded after the information is processed.

3. **In-Person:** When processing a credit card transaction into the POS, it must be processed in full view of the customer. Staff is prohibited from writing or storing card information. Credit card information should be processed directly into the system while customer is present at location. Security controls must be in place when handling in-person transactions.

4. **Via Fax or Email:** Credit card information may not be accepted via fax, email, or any other unsecure communication medium. If a customer does send an email with their card information, the information should be deleted immediately from all email folders. The customer should also be contacted to indicate that the information has been deleted and the transaction has not been processed. The staff member can then work with the customer to complete the transaction in an authorized manner. A PCI incident response ticket at https://nsd.miamidade.gov/sr/pciincrep must be initiated in order for the Information Technology Department (ITD) to verify that the email(s) have been securely deleted.

5. **Internet:** Transactions shall be processed via the County’s Gateway managed by ITD and no cardholder information shall be saved/stored. Third Party payment application systems require compliance with the section IV, “Contract Language for Credit Card Payment Systems”.

Page 3 of 19
II. Accounting Controls

A. Chargeback Processing:
   1. There are several mediums for receiving chargebacks, i.e. fax, internet and mail. If chargeback notices are received via fax, the fax shall be in a physically secure location, only appropriate staff may have access, and documents shall be securely cross-shredded as soon as they are processed. If chargebacks are received via internet, it must be received through a secured access and only the last four digits of the credit card number should be visible for processing. In addition, if full credit card numbers are visible, the information must be deleted immediately, and an incident response ticket must be initiated. The vendor must be contacted and informed if full credit card numbers are visible in documents sent.
   2. If the fax machine has a memory card, special care should be taken to clear the memory card from the fax machine daily.
   3. Staff member issuing chargebacks may not also conduct regular sale transactions and/or have reconciliation/journal entry duties.
   4. Only staff with a level of an Accountant 2 or above will be approved for chargeback access.
   5. Supervisors shall review and approve each chargeback.

B. Refunds/Voids/Credits:
   1. There are many options for processing refunds. Caution should be taken to ensure that the full credit card number is not stored if received from the credit card provider. If at any moment full credit card numbers are received, the information should be securely cross-shredded.
   2. Staff member issuing refunds may not also conduct regular sale transactions and/or have reconciliation/journal entry duties.
   3. Only staff with a level of an Accountant 2 or above will be approved for refund access.
   4. Supervisors shall review and approve each refund.
   5. Refunds may not be issued by cash or check. All refunds must be made to the original form of payment (same credit card used in the sale transaction).
C. Reconciliation

1. As each department with physical credit card terminals closes their batches at end of the day, a data file is created with our credit card processor. This data file is sent electronically to our processor. POS terminals must be closed out each day with a batch settlement process. Training will be provided upon initial set up to access system reports.

2. A detailed reconciliation process shall be done at least monthly, which shall include reports (Reports of Collection (ROC)) used to record the transactions into FAMIS and the location’s Index Code. Maintain copies for audit review.

3. The ROC will be reviewed and approved by the department supervisor and shall be delivered to the Finance Department, Controllers Division, Input/Output Section.

III. Terminals (Point of Sale (POS) Equipment)

Terminals shall be stored in a physically secure location when not in use. There shall be a documented and periodic review process in place performed at least quarterly to detect for any tampering of equipment (unauthorized Payment Card Skimmers) and a log must be maintained of the periodic review. Payment Identification Numbers (PINs) must be activated on the terminals immediately upon delivery for each individual user. PIN numbers should never be shared and shall be updated semiannually.

Wireless terminals shall connect directly to County’s approved processor via Cellular carrier (i.e. Sprint, AT&T, etc.). Many portable devices that attach to tablets, smartphones, etc. are not PCI compliant and should not be used. The Finance Department Cash Management Division must be contacted to order credit card equipment.

Terminals may NOT be connected to the Network, unless these are pre-approved Point-to-Point Encryption (P2PE) devices. (Contact Finance’s Cash Management Division or PCI Compliance team for additional information on P2PE services) and pricing.

Broken terminals shall be reported to the Finance Department Cash Management Division for replacement/disposition instructions.
IV. Payment Card Industry Data Security Standards

The PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common-sense steps that mirror security best practices. Noncompliance to these standards can result in significant fines assessed to the County and may result in loss of the ability to accept credit cards.

In order to ensure compliance with PCI DSS, departments that accept credit card payments must complete an annual PCI Self-Assessment Questionnaire and Attestation of Compliance. The County must conduct, quarterly vulnerability scans, and both an annual formal risk assessment, and penetration test to identify threats and vulnerabilities to the secure Credit Card Network (CCN). This policy must be reviewed annually and updated when the credit processing environment changes. The Finance and Information Technology Departments jointly monitor compliance and work with other departments to provide training and information to comply with these requirements.

Below is a high-level overview of the PCI DSS requirements. The complete standards are accessible at the PCI Security Council website. Also refer to the Miami Dade County Payment Card Industry Executive Charter and Compliance Policy 332.

<table>
<thead>
<tr>
<th>Build and Maintain a Secure Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</td>
</tr>
<tr>
<td>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect Cardholder Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 3: Protect stored cardholder data.</td>
</tr>
<tr>
<td>Requirement 4: Encrypt transmission of cardholder data across open, public networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintain a Vulnerability Management Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 5: Use and regularly update anti-virus software or programs.</td>
</tr>
<tr>
<td>Requirement 6: Develop and maintain secure systems and applications.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement Strong Access Control Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 7: Restrict access to cardholder data by business need to know.</td>
</tr>
<tr>
<td>Requirement 8: Assign a unique ID to each person with computer access.</td>
</tr>
<tr>
<td>Requirement 9: Restrict physical access to cardholder data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regularly Monitor and Test Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 10: Track and monitor all access to network resources and cardholder data.</td>
</tr>
<tr>
<td>Requirement 11: Regularly test security systems and processes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintain an Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 12: Maintain a policy that addresses information security for all personnel.</td>
</tr>
</tbody>
</table>
V. Contract Language for Credit Card Payment Systems

This section is applicable when purchasing or upgrading any systems that store, process or transmit payment card data. This entire section shall be included in all Request for Proposals, Contracts, and/or agreements and must be agreed by the selected vendor for the systems being procured/implemented.

If at any time any of the components, including but not limited to the vendor’s system, equipment, hardware, software or policies, becomes non-PCI compliant, vendor is responsible for all costs related to upgrading the system so that PCI compliance is maintained throughout the term of the agreement.

a. The Vendor confirms its knowledge of and commitment to comply by providing the following proof that Vendor’s devices/applications/processes meet current, published, PCI compliance requirements:

1. Vendor’s current annual PCI Compliance certification if applicable. The County has right to audit vendor compliance by requesting copies of the vendor PCI compliance certifications at any time.

2. During an installation or a major system upgrade, the vendor must provide implementation manuals and detailed diagram(s) that show all cardholder data flows across MDC’s systems and networks, the internet and the processor network.

3. Vendor Form – Payment Application(s) (refer to section A) – Only applicable to the vendor who is installing the product in County environment.

b. Vendor shall resubmit the aforementioned passing, updated, completed and signed PCI compliance documents annually to the County. Furthermore, the Vendor shall update their solution, when required, to remain compliant with all changes to the PCI standards and requirements by the implementation dates mandated by the PCI Security Council and remediate any critical security vulnerabilities within 30 days of identification.

c. Sensitive Authentication data and Primary Account number shall not be stored by the vendor application at any point, even if masked. Any other Card holder data should not be stored by the vendor application unless it is absolutely needed for County’s operations.

d. POS (Point of Sale) and Retail transactions must be routed directly to Miami-Dade County’s merchant provider (ELAVON) and must be EMV compliant. All POS and Retail transactions must be capable of accepting NFC (near field communications) payment methods such as Google Wallet, ApplePay, or Samsung Wallet.

e. Systems that utilize MDC network for payment processing must be a validated PCI Point-to-Point Encryption (P2PE) solution and transactions routed through
our approved County merchant processor. Exceptions to using Elavon P2PE solutions shall require written justification by Department, including a cost/benefit analysis, and require written approval by both the Finance Department Director and Chief Information Officer.

f. Internet transactions must be routed through Miami-Dade County’s Internal Payment Gateway (Payment Card and eCheck). Exceptions to using Miami-Dade County’s Internal Payment Gateway shall require written justification by Department, including a cost/benefit analysis, and require written approval by both the Finance Department Director and Chief Information Officer.

g. Transactions processed through the Miami-Dade County Internal Payment Gateway are prohibited from accepting / processing PIN numbers for security reasons. Debit card transactions must be processed as credit card transactions. Miami-Dade County provides three basic services that allow Contractor applications to interact with its Payment Gateways:

1. Web-based Credit Card Transaction Service
2. Web-based ACH (e-Check) Transaction Service
3. Recurring Payment Service (for monthly or yearly recurring payments). This service will allow merchants to develop recurring credit card payments on behalf of their payers. This is a SOAP Web Service, and Miami-Dade County will provide the service WSDL and the necessary documentation. The Recurring Payment Service is PCI-compliant, and all the sensitive credit card data is stored offsite in the County’s clearinghouse.

There are two different ways that a merchant customer can handle the Credit Card or ACH (e-Check) transaction processing;

a. Option #1:

The Contractor application interfaces directly with Miami-Dade County’s Payment Gateway via a RESTful web-service. Miami-Dade County will provide the XML schemas to all basic services: web payment processing, void, refund, and recurring payments. Miami-Dade County will also provide all the necessary URLs for these services, as well as, documentation detailing fields and response codes. All services will respond with the same XML receipt.

This solution will require the client application to fully interact with Miami-Dade County’s Payment Gateway, reacting to processing and system errors. Even though this solution requires more development and integration from a vendor, it will offer the greatest flexibility and customization level. This option also requires for the vendor application to be hosted on a server inside the County’s
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

managed network, since Miami-Dade County’s Payment Gateway is not accessible from the Internet. If the application is outside of the County's Managed network, Miami-Dade County can develop a Payment Module Application (option #2) that will service the vendor’s application.

b. Option #2:

A vendor application will utilize a Payment Module Web Application developed and maintained by Miami-Dade County. This solution can be a standard web application, a mobile web application, or both. A link will be provided on the vendor application that sends payers to the Payment Module Application. For example, once the payer has selected the items to purchase (from the vendor's application), there would be a “Pay Now” button that will redirect the payer to the Miami-Dade County Payment Module via HTTPs post, carrying all the necessary data to begin the payment process (User ID, Amount, etc.). This requires only minor development effort on the vendor side. The vendor will agree on custom fields to be passed to the Miami-Dade County Payment Module via HTTP protocol over TLS 1.2 or higher (only secure connections are accepted; SSL protocol is not accepted). In turn, the Miami-Dade County Payment Module will collect the payment information and process the transaction via the Miami-Dade County Internal Payment Gateway. Results will be posted back (post back URL is provided by the client application) to the vendor application. This solution will not require the client application to be hosted in the County's managed network. The Miami-Dade County Payment Module handles all processing and system errors, simplifying the integration effort on the vendor side.
A. Vendor Form

Vendor Form – New Payment Applications

<table>
<thead>
<tr>
<th>Vendor Information</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Company Name:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Primary Contact:</td>
<td>Job Title:</td>
<td></td>
</tr>
<tr>
<td>E-mail:</td>
<td>Telephone:</td>
<td></td>
</tr>
<tr>
<td>Business Address:</td>
<td>City:</td>
<td></td>
</tr>
<tr>
<td>State/Province:</td>
<td>Country:</td>
<td></td>
</tr>
<tr>
<td>Postal Code:</td>
<td>URL:</td>
<td></td>
</tr>
</tbody>
</table>

PA-DSS Validated Payment Application

<table>
<thead>
<tr>
<th>Application Details</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Location(s) where application was installed</td>
<td>Type of Application installed</td>
<td>Number of Systems installed</td>
</tr>
</tbody>
</table>

Implementation Approach

This implementation statement confirms that:

- The validated payment application was installed in accordance with the PA-DSS Implementation Guide. Respond Yes or No.
- If response is “No”, please provide a brief explanation.

PA-DSS Implementation Guide and Training Materials

- Date and version of the PA-DSS Implementation Guide used during the installation of the payment application.
- Provide a copy of the Implementation Manuals.
Remote Access
Is remote access into their network configured as follows:
| Remote access to the payment application requires two factor authentication? |
| Remote access implemented securely? |

Network Configuration
Are any external connections required by the payment application?

Sensitive Authentication Data (SAD)
Is the application configured to ensure that sensitive authentication data (including full track data, card verification codes/values and PIN or PIN Block) is not stored after authorization, even if encrypted?

Accounts and Passwords
Is strong authentication configured for all application administrative accounts and for all application accounts with access to cardholder data?

Wireless
Does the payment application use wireless technology?

Completed by: ________________________________

Department Review:

Name: ________________________________

Title: ________________________________

Phone #: ________________________________ Date: ________________________________

Copy of this document must be provided to Finance along with Memorandum requesting approval for MID.
VI. PCI Liaison

Department Directors shall establish a PCI Liaison (Accountant 4 or above) to oversee the PCI Compliance and provide an appropriate replacement as may be required.

The liaison will be responsible for monitoring departmental PCI Compliance, reviewing and updating departmental documentation, and ensuring that appropriate staff is trained. All staff involved with the credit card processing functions shall have appropriate training, which includes the credit card policy, information security, and other relevant policies. Department procedures, inventory, merchant identification report, diagrams, third party payment application certifications will need to be reviewed/updated on a yearly basis. In addition, liaison will need to work with the Finance and Information Technology departments to coordinate and ensure timely preparation, review and approval of the Self Attestation Questionnaires (SAQs) and Attestation of Compliance (AOC) forms.

A current list of PCI Liaisons can be accessed through the following link: http://intra.miamidade.gov/finance/payment-card-industry.asp

VII. Approvals

Request for new credit card services will require a memorandum approved by the Department Director (refer to section VIII, “Procedures for new credit card services and equipment”). Annual updates of credit card procedures, training reports, SAQs and AOCs shall be signed/approved at a minimum by the department's PCI Liaison and the Department Director.

It is the Departments responsibility to ensure that all personnel responsible for processing, reviewing, reconciling and approving credit card transactions shall be provided a copy of these procedures and the Miami Dade County Payment Card Industry Executive Charter and Compliance Policy 332.

VIII. Procedures for Requesting New Credit Card Services and Equipment

When requesting approval for implementing new credit card services departments shall explain the type of service, application, and procedures that will be implemented. The following are required:
I. Memorandum from the Department Director,

II. Credit Card Procedures *(using approved template in section VIII.A)*,

III. Diagram(s) *(environment)*,

IV. Merchant Identification Report,

V. Inventory Report *(hardware, software)*,

VI. PCI Certification *(if using a third-party vendor application)*

I. The memorandum shall include the following:

1. Description of the services, products, etc., being sold. Include information on any related Statutes, Administrative Orders, Implementing Orders, and/or business needs identified to justify the need for accepting credit cards.

2. Describe the method used to process transactions (WEB, credit card machine, Third Party Vendor software, P2PE service etc.) and if the transactions will be processed through the County’s Gateway or directly to payment processor, Elavon. Note: County Policy is to have all credit card transactions processed via the County Gateway unless an exception is approved by the Finance Director or Director’s designee. All third-party payment systems shall be PCI compliant. Departments selecting P2PE services must complete P2PE Pricing Sheet available through Finance’s Cash Management Division. Both the Finance Department Compliance Section and ITD shall review and approve PCI compliance prior to system purchase. Vendors are required to maintain PCI compliance throughout the life of the contract and be in compliance with section IV, “Contract Language for Credit Card Payment Systems.”

3. Acknowledgement that staff responsible for any portion of the credit card environment are aware of and fully complies with PCI Security Standards *(https://www.pcisecuritystandards.org/)* and Miami Dade County Payment Card Industry Executive Charter and Compliance Policy 332 and Credit Card Acceptance and Processing Procedures 333.

4. A clear statement that sensitive authentication data (Full Track Data, CVV/CVS and PIN) is not stored physically or electronically at the location or in any systems component.

5. Include request for new equipment (terminal-Point of sale machines), who will be the contact and where they will be shipped.

6. Memorandum should be signed and approved by the respective Department Director.
II. **Credit Card Procedures** - Follow the guidelines established in these procedures and use the approved template (refer to section VIII. A).

III. **Diagrams** - Provide diagrams of the credit card environment. Include existing environment if already using other credit card applications.

IV. **Merchant Identification (MID) Report** - Provide a list of all MIDs currently being used. The report can be found in the PCI Sharepoint drive and must be updated annually or when requesting a new payment process.

V. **Inventory Report** – Provide an inventory report of all the hardware that will be used in the credit card environment. The Information Security Office at ITD can be contacted for assistance with this report. The report can be found in the PCI Sharepoint drive and must be updated semi-annually or when there is a change.

VI. **PCI certification** – Departments must retain vendor PCI related documentation for third-party payment systems; i.e. Payment Application Data Security Standard PA-DSS or Attestation of Compliance (AOC). In addition, for departments selecting P2PE services, Elavon’s PCI validation can be found in the PCI website.

All required documents shall be submitted to the Finance Director/Finance Deputy Director by submission through the Cash Management Division for review and approval.

**Approval process:**

1. A review of the documents will be completed by the Finance and ITD to ensure compliance with respective procedures and PCI guidelines. If all is acceptable, the Finance Director or designee will approve the request and the merchant and user forms will be sent to the respective PCI Liaison for processing.

2. The Department will need to contact ITD and schedule a meeting if programming is needed and to provide pricing. If the project is agreed to, ITD provides the Department with e-Commerce Merchant Account and User ID setup forms. If only a Terminal (Point of Sale) device is needed, contact the Finance Department Cash Management Division after discussion with ITD on device options, written approval from Finance and ITD are required for non-approved devices to ensure PCI compliance. Departments must provide PCI certification for review and determination.

3. Setup forms are signed by the requesting Department Director, or designee, and Finance Compliance Section, approving the set-up of both
the merchant account (with the merchant processing company) and the Gateway account (with ITD). Please note, ITD will not setup new accounts and/or new users unless signed set up forms are received.

4. Cash Management Division notifies the merchant processor of the request to open an account and the processor provides an Add Location Form and/or Tokenization Enrollment Form. Cash Management Division forwards the form to the Department for information to be filled in, such as address, other contact information, estimates for monthly/yearly dollar volume, average ticket size, equipment needs, etc.

5. The Department fills in all necessary information (except bank information) and returns the form (via email) to Cash Management Division, who will fill in the bank information and forward to the processor company.

6. Departmental PCI Liaisons should send an email to Cash Management Division requesting the equipment or describing the services needed. For replacement of existing equipment requests or requesting pre-approved equipment, the following information should be included:
   a) Type of equipment and/or P2PE services;
   b) Merchant ID number to be used;
   c) Department name;
   d) Shipping address;
   e) Attention to; and
   f) Include if needed, a request for Call Tags to be sent to the Department. Call Tags are used to return broken, outdated, etc., equipment back to the merchant processing company for proper disposal.

7. The processor notifies the Cash Management Division when the account is opened. Cash Management Division will, in turn, notify the Department that the account is setup as well as the Merchant ID (MID) number assigned by the payment processor company, and will provide a link to the Merchant Operating Guide (MOG) provided by the merchant processor.

8. Cash Management Division will coordinate with the Department and the merchant processor to evaluate various factors that may affect the service, such as dollar volume, average ticket size, etc.

9. The Department should contact the Finance Department Bank Reconciliation Unit Supervisor (305-375-5167) for information on journal entry, reports, etc., that may be needed for reconciliation purposes.
A. Template for requesting new and updated services:

Miami Dade County (Insert Department Name)
Credit Card Processing Procedures for:
(Insert name of process)

I. Background & Overview:

1. Description of the services, products, etc., being sold. Include information on any related Statutes, Administrative Orders, Implementing Orders, and/or business needs identified to justify the need for accepting credit cards.

2. Method used to process transactions (WEB, POS, County Gateway, Third Party Vendor software, etc.) Note: County Policy is to have all credit card transactions processed via the County’s Gateway unless an exception is approved by the Finance Director or Director’s designee. If any third-party systems are used include their role in processing transactions. Also, confirm that a written confirmation has been received from the vendor that they are PCI compliant and will maintain PCI compliance throughout the length of the contract.

3. State that the processing location is aware of and fully complies with PCI Security Standards (https://www.pcisecuritystandards.org/) and MDC procedures #332 Payment Card Industry Executive Charter Compliance Policy and #333 Credit Card Acceptance and Processing Procedures.

4. A clear statement that no credit card information sensitive authentication data (Full Track Data, CVV/CVS and PIN) is stored physically or electronically at the location or in any systems component.

II. Handling Credit Card Information:

Describe the credit card environment. Specify details for each of the following methods (including reports used, processing cutoff times, titles of responsible staff, etc.). State that protecting credit card is essential and physical access to data systems that house, process or transmit cardholder data is appropriately restricted:

1. **Via phone:** Confirm that staff is prohibited from recording credit card conversation(s) and writing credit card information, which should be entered directly to the system as it is received from the customer. Explain security controls (secure location, staff access to information, etc.) Ensure conversations are taken in a secured location not audible to other staff members or customers.

2. **Via U.S. Mail:** Every effort should be made not to accept credit card information via U.S. mail. The policy should clearly describe the process for securing the mail (secured room, security camera’s etc.), which staff member has access to the mail (restricted to a business need to know, are staff screened? etc.), and the cross shredding of the card information as soon as it is processed.
3. **In-person:** Explain process when entering credit card information into POS and how in-person transactions are handled; transactions must be processed in full view of the customer. Confirm that staff is prohibited from writing down or storing credit card information. Explain security controls for the location.

4. **Via Fax or Email:** Credit card information may not be accepted via fax, email, or any other unsecure communication medium. If a customer does send an email with their card information, the information should be deleted immediately from all email folders. The customer should also be contacted to indicate that the information has been deleted and the transaction has not been processed.

5. **Internet:** Expand on the role of any third (3rd) party vendors, confirm that transactions are processed via the County’s Gateway managed by ITD, and confirm that no Cardholder information is saved/stored at the location.

### III. Chargeback processing:

a. There are several mediums for receiving chargebacks, i.e. fax and mail. Explain how chargebacks are received. If chargeback notices are received via fax, confirm that the fax must be in a physically secure location, only appropriate staff has access, and documents are securely cross-shredded as soon as they are processed. If chargebacks are received via internet, it must be received through a secured access and only the last four digits of the credit card number should be visible for processing.

b. If the fax machine has a memory card, special care should be taken to clear the memory card from the fax machine daily. If the chargebacks are received via email and there is credit card information received, explain that the information will be immediately deleted.

c. Confirm that the staff member issuing chargebacks does not also conduct regular sale transactions and/or have reconciliation/journal entry duties.

d. Only staff with a level of an Accountant 2 or above will be approved for chargeback access; the name and title of those staff members will need to be provided and updated annually.

e. Supervisors must review and approve each chargeback; the name and title of those supervisors will need to be provided and updated annually.

### IV. Refunds/Voids/Credits:

a. Describe in detail each step of the process including any reports printed, what type of cardholder information is on the reports, whether the reports are downloaded to electronic format and stored, etc. Caution should be taken to ensure that the full Primary Account Number (PAN) is not stored if received from the credit card provider. Explain if at any moment full credit card numbers are received, the information should be securely cross-shredded.

b. Confirm that the staff member issuing refunds does not also conduct regular sale transactions and/or have reconciliation/journal entry duties.
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

c. Only staff with a level of an Accountant 2 or above will be approved for refunds access. The name and title of those staff members will need to be provided and updated annually.

d. Supervisors must review and approve each refund; the name and title of those supervisors will need to be provided and updated annually.

e. Confirm that refunds will only be issued to the customer’s original credit card that the sales transaction was initiated with. Refunds cannot be processed by cash or checks.

V. Reconciliation:

a. POS Terminals shall be closed out each day with a batch settlement process.

b. A detailed reconciliation process must be done at least monthly. Include a description of the reconciliation process, including reports [Reports of Collection (ROC) etc.] used to record the transactions into FAMIS and credit the location’s Index Code. Maintain copies for audit review.

c. Confirm that the ROC will be reviewed and approved by the department supervisor and is delivered to the Finance Department, Controllers Division, Input/Output Section.

VI. Terminals:

a. Provide a report of an inventory list of each terminal at the location including model number, serial number, and last 4 digits of the Merchant ID.

b. Confirm that a unique PIN will be used by each staff member using the terminal and that staff understands that PINs cannot be shared.

c. Confirm that there is a documented and a quarterly review process in place to detect for any tampering of equipment (unauthorized payment card skimmers) and that a log maintained of the quarterly review.

d. Provide physically secure location where terminal will be stored when not in use.

e. Confirm that terminals will not be connected to the network.

f. If using a wireless terminal, confirm the cellular carrier being used and that it has been approved through the County’s approved processor.

g. Confirm that Cash Management will be contacted for instruction on disposition/replacement of all terminals.

VII. PCI Liaison: On a yearly basis, the department will need to complete and sign (by the Department Director) a self-assessment questionnaire (SAQ) and Attestation of Compliance (AOC) form, as mandated by the Payment Card Industry (PCI) Data Security Standard (DSS). The Policy should also contain the following:

a. The Name and title (Accountant 4 or above) of the PCI Liaison to oversee the credit card processing and work with Finance and ITD on PCI compliance and training.

b. Include a statement that this policy will be reviewed/updated upon changes to the credit card environment and/or annually.
c. Include a statement that all staff involved with the credit card processing functions will be trained and provided with a copy of MDC Payment Card Industry Executive Charter and Compliance Policy and the Credit Card Acceptance and Processing Procedures (Procedure Number 332 and 333). Annual certification of training completion must be submitted to the Finance Department and approved by the respective department Director.

VIII. **Summary of documents for submission to the Finance Department:**

1. Memorandum from the Department Director
2. Credit Card Procedures (using Template for New and Updated Credit Card Procedures)
3. Diagrams
4. Merchant Identification Report
5. Inventory Report
6. PCI Certification

*Note: Annual updated require submission of items above.*

IX. **Approvals:** The procedures must be signed/approved by the Department's PCI Liaison and the Department Director. A statement must be included that the department has read and will comply with the MDC Payment Card Industry Executive Charter and Compliance Policy and the Credit Card Acceptance and Processing Procedures (Procedure Number 332 and 333).

______________________________________________________________________________
Department PCI Liaison .............................................................................................................. Date

______________________________________________________________________________
Department Director .................................................................................................................. Date