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

V. Payment Card Industry Data Security Standards

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 contracted credit card payment processor vendor. Departments may not contact the vendor directly for new equipment.

A. Handling Credit Card Information

In accordance with PCI DSS, all employees involved in processing credit card transactions and the support of the cardholder data environment (process, reconcile, system support, etc.) must be trained annually on the appropriate procedures. The County offers online training and each department is responsible for ensuring that respective employees take the training.

Protecting cardholder data is essential; thus, every effort shall be made NOT to store cardholder information in any form. Any physical access to data or systems that house, process, or transmit cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted.
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 and writing card information, which should be entered directly into the system as soon as it is received from the customer.

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. **Via Fax or Email:** Credit card information should not be accepted via fax, email, or 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 (contact your **PCI Liaison**) must be initiated in order for the Information Technology Department (ITD) to verify that the email(s) have been securely deleted.

4. **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”.
II. **Accounting Controls**

A. **Chargeback Processing:**
   1. 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 cross shredded as soon as they are processed.
   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. The name and title of those supervisors will need to be provided and updated annually.

B. **Refunds/Voice/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.
   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; the name and title of those supervisors will need to be provided and updated annually.
   5. If payment was received from the customer by use of a credit card, any refund is to be made to the same credit card originally used. Cash or checks are not acceptable reimbursement methods for credit card sales, as they are not accepted as proof of a refund by the merchant bank.

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. Training will be provided upon initial set up to access system reports.
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

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 shall be delivered to the Finance Department, Controllers Division, Input/Output Section.

III. Terminal (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 maintained of the periodic review. Individual user Payment Identification Numbers (PINs) must be activated on the terminals immediately upon delivery. 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.

Terminals may NOT be connected to the Network.

Broken terminals shall be reported to the Finance Department Cash Management Division for replacement/disposition instructions.
IV. 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 for the application and by vendor selected.

The Contractor shall comply with the Payment Card Industry Security Standards in effect and at all times throughout the term of this agreement. 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 Contractor confirms its knowledge of and commitment to comply by providing the following proof that Contractor’s devices/applications/processes meet PCI compliance requirements:

1. Contractor’s current annual PCI Compliance certification. The County has the auditing right to request copies of the PCI compliance certifications at a later time.

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

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

b. Contractor shall resubmit the aforementioned passing, updated, completed and signed PCI compliance documents annually to the County. Furthermore, the Contractor 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. 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.

f. 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
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

Metronet, since Miami-Dade County’s Payment Gateway is not accessible from the Internet. If the application is outside the Metronet, 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 Metronet. 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

MIAMI DADE COUNTY

VENDOR FORM – PAYMENT APPLICATIONS

Vendors providing payment applications/services to Miami-Dade County must be in accordance with PA-DSS Requirement #13. Vendors must fully complete this form and submit their official compliance documentation to Miami-Dade County. Please refer to the Credit Card Payment System vendor requirements document for further information.

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

<table>
<thead>
<tr>
<th>PA-DSS Validated Payment Application</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Application Name:</td>
<td></td>
</tr>
<tr>
<td>Application Version Number:</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Application Details |  |</p>
<table>
<thead>
<tr>
<th>Location(s) where application was installed</th>
<th>Type of Application installed</th>
<th>Number of Systems installed</th>
<th>Date Installed</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Implementation Approach</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This Implementation Statement confirms that:</td>
<td></td>
</tr>
<tr>
<td>The validated payment application was installed in accordance with the PA-DSS Implementation Guide. Respond Yes or No. If response is &quot;No&quot;, please provide a brief explanation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PA-DSS Implementation Guide and Training Materials</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and version of the PA-DSS Implementation Guide used during the installation of the payment application. Provide a copy of the Implementation Manuals.</td>
<td></td>
</tr>
</tbody>
</table>
### Remote Access

<table>
<thead>
<tr>
<th>Is remote access into their network configured as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access to the payment application requires two-factor authentication?</td>
</tr>
<tr>
<td>Remote access implemented securely?</td>
</tr>
</tbody>
</table>

### 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.*
V. 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>
VI. PCI Liaison

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

The liaison will be responsible for monitoring departmental PCI Compliance 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 by the department’s PCI Liaison and the Department Director.

Please ensure that all personnel responsible for processing, reviewing, reconciling and approving credit card transactions are 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 will be required:
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

1. Memorandum from the Department Director
2. Credit Card Procedures *(using approved template in section VIII.A)*
3. Diagram(s) *(environment)*
4. Merchant Identification Report
5. Inventory Report *(hardware, software)*
6. PCI Certification *(if using a third-party vendor application)*

Once the memo and the procedures have been signed and approved by the respective Department Director, all required documents shall be submitted to the Finance Director/Finance Deputy Director by submission through the Cash Management Division for review and approval. Upon review and approval, departments will be contacted with additional information for processing. The cost of processing credit cards will be charged to the respective department. In order to comply with the PCI regulations, procedures and documentation will need to be updated annually with corresponding approvals.

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, etc.) and if the transactions will be processed through the County’s Gateway. 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. 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 MDC procedures #332 and #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.
CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

Along with the memorandum include the following as attachments:

1. **Credit Card Procedures** following the guidelines as established in this procedure #332 and using the approved template (refer to section VIII. A).
2. **Diagrams** of the credit card environment, include existing environment if already using other credit card applications.
3. A **Merchant Identification (MID) Report** updated with all MIDs currently being used; if this is the department’s first credit card application, a new MID will be provided.
4. 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. This report will need to be updated on a monthly basis.

**Approval process:**

1. A review of all 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 will approve the request and the merchant and user forms will be sent to the respective PCI Liaison.

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 (CM) Section after discussion with ITD on device options.

3. Setup forms are signed by the Department Director, Deputy Finance Director, and CM Director, approving the set-up of both the merchant account (with the merchant processing company) and the Gateway account (with ITD).

4. CM notifies the merchant processor of the request to open an account and the processor provides an Add Location Form. CM 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 CM, who will fill in the bank information and forward to the processor company.
6. Departments should send an email to CM requesting the equipment or describing the services needed. For equipment requests, the following information should be included:

a) Type of equipment;
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 CM when the account is opened. CM 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. CM 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. Approved Template for requesting new services can be found at: http://intra.miamidade.gov/finance/payment-card-industry.asp