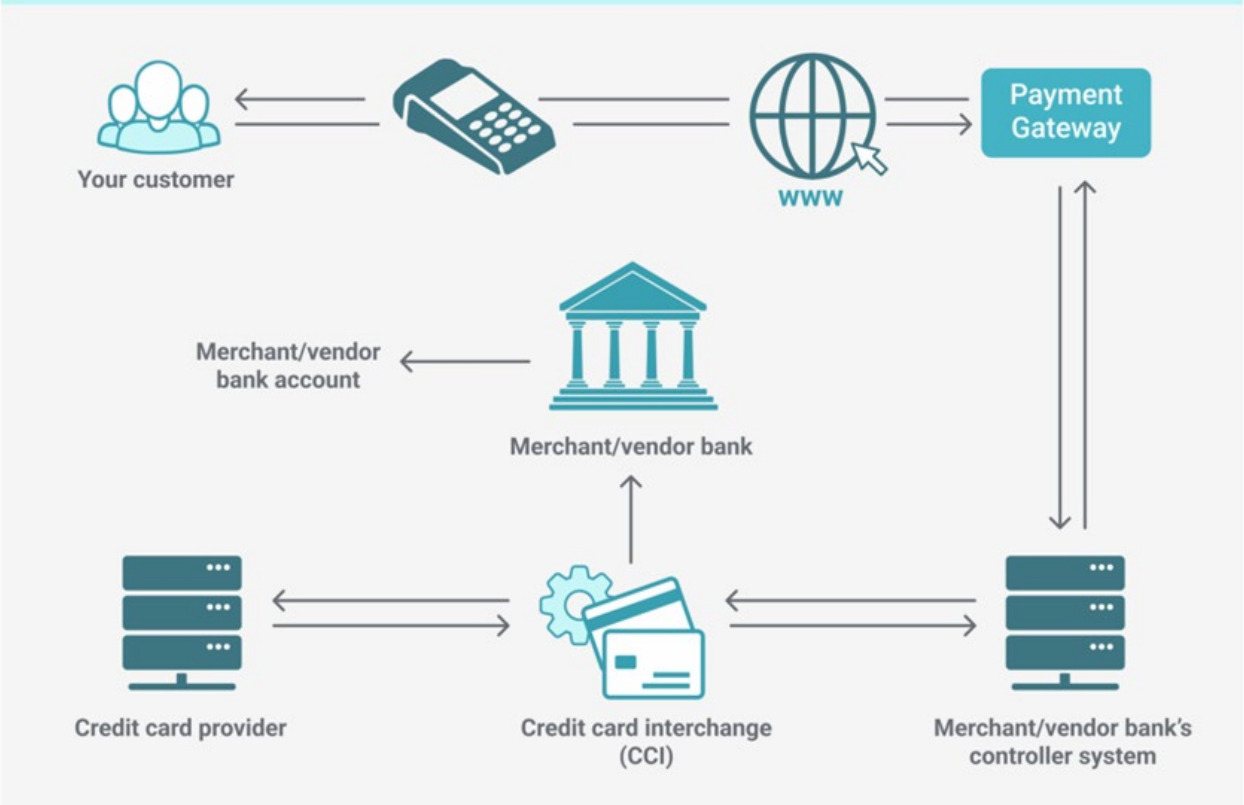
Clerk of the Court and Comptroller

of

Miami Dade County

333: Credit Card Acceptance and Processing Procedures

PCI Team | 11/1/25 | No. 333


Your customer
Payment Gateway
WWW
Merchant/vendor bank account
Merchant/vendor bank
Credit card provider
Credit card interchange (CCI)
Merchant/vendor bank's controller system

INTRODUCTION

The purpose of these procedures is to provide guidance for accepting credit card payments for services throughout Miami-Dade County departments and Constitutional Offices. This policy provides guidance on the Payment Card Industry (PCI) Standards which assist in mitigating the risk of credit card fraud and data security breaches, while maintaining a secure environment for all card transactions.

Table of Contents

I. Revisions to Procedure:

This section documents the revisions made to this procedure since the last approved version dated October 2024.

Effective Date	Version	Description	Pages
October 2025	333.6.0	Updated cover page	cover
October 2025	333.6.0	Updated name of department and logos	cover, i–23
October 2025	333.6.0	Updated name of Information Technology Department	2-23
October 2025	333.6.0	Updated name of PCI Team	2-23
October 2025	333.6.0	General grammatical changes	2-23
October 2025	333.6.0	Updated title of procedures in Section III “Applicable Policies and Procedures	2
October 2025	333.6.0	Updated “Department/CO” to “Miami-Dade Entity”	2-23
October 2025	333.6.0	Clarified verbiage in “Via Fax or Email” channel in Section IV (A) “Handling Credit Card Information”	4, 20
October 2025	333.6.0	Updated verbiage and clarified frequency of POS Terminals inspections in Section VI “Point of Sale Devices”	6
October 2025	333.6.0	Clarified verbiage on “PAN Masking” in Refund Processing	6, 22
October 2024	333.6.0	Clarified verbiage in Contract Language in Section VIII (A)	9
October 2025	333.6.0	Reformatted Contract Language in Section VIII (A)	10
October 2025	333.6.0	Expanded on new credit card process documentation in Section VIII (B)	13
October 2025	333.6.0	Clarified verbiage on new credit card process documentation in Section VIII (B)	14-17
October 2025	333.6.0	Expanded verbiage in the Section XI “Template for Credit Card Procedures Request”	19-23

II. Scope:

All employees, contractors, and vendors involved in processing credit card transactions and/or supporting the cardholder data environment (e.g., processing, reviewing, reconciling, approving, system supporting, etc.) are subject to the terms of this procedure.

III. Applicable Policies and Procedures:

- Payment Card Industry Executive Charter and Compliance Policy (Policy #332)
  https://www.miamidade.gov/managementandbudget/library/procedures/332.pdf
- Miami Dade County Enterprise Information Security Policy Manual
  https://intra.miamidade.gov/finance/library/security-policy-manual.pdf
- Payment Card Industry Data Security Standards Incident Response Plan
  https://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf
- Miami-Dade County Identity Theft Prevention Program (Red Flags-Resolution R-580-10
  https://www.miamidade.gov/govaction/legistarfiles/Matters/Y2010/101045.pdf
- Clerk of the Court and Comptroller of Miami-Dade County Credit Card Processing Procedures for Working Remotely (Procedures #334)
  https://intra.miamidade.gov/finance/library/334-credit-card-work-remotely.pdf

IV. Acceptance and Processing

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

New services will be requested through CFO, in accordance with these procedures and the completion of *Section XI – Template for Requesting New/Updated Services and Equipment*. The cost of equipment and processing credit card transactions will be paid from the Miami-Dade Entity funds. Technology implementation must be in accordance with the Payment Card Industry Data Security Standards (PCI DSS) as noted in Sections VII and VIII of these procedures.

Miami-Dade Entities must use the credit card payment processor(s) under contract with the Clerk of the Court and Comptroller (COCC). The CFO's Cash Management Division and the Administrative & Compliance Services Division will assist Miami-Dade entities to obtain new services and equipment working with the Clerk's contracted credit card payment processor. **Miami-Dade Entities shall not contact the payment processor directly for new equipment or services.**

A. Handling Credit Card Information

In accordance with PCI DSS, Req. 12.6.3, 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. COCC offers an annual in-person training each January in addition to mandatory PCI online training courses that each Miami-Dade Entity is responsible for ensuring their respective employees complete. Refer to COCC's PCI Charter #332, *Section C. Required Information Security & PCI 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 to not provide the opportunity for persons to access and/or remove devices, data, systems, or hardcopies. If credit card information is visible during any type of processing, it must be masked and only display the last four digits of the Primary Account Number (PAN). The masking or truncation of the credit card account information shall also be in accordance with the Federal Fair and Accurate Credit Transaction Act (FACTA). Only personnel with a legitimate business need may be authorized access beyond the Bank Identification Number (BIN) and last four digits of the PAN.

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

1. **Via the phone:** Staff is prohibited from recording credit card phone calls/conversation(s) or writing full credit card number(s), which should be entered directly into the system or Point-of-Sale (POS) terminal as soon as it is received from the customer. Security controls must be in place when handling payments over the phone. Phone payments must be processed in secure, private areas. Staff must not have access to personal devices during transactions, and conversations must not be audible to others. (Refer to Section IV (B) for additional information when Working Remotely).

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, Miami-Dade Entities must secure the documents received. It is recommended that mail containing credit card data should be opened and logged in a secure room with cameras, restricting access to credit card data. All card data must be securely cross shredded after processing.

3. **In-Person**: When processing a credit card transaction into the system or POS terminal, 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 or POS terminal 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 must 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/cross shredded, and the transaction has not been processed. The staff member can then work with the customer to complete the transaction in an authorized manner.

5. **Internet:** Transactions shall be processed via the County's Payment Gateway managed by the Communications, Information & Technology Department (CITD) and no cardholder information shall be saved/stored. Third Party payment application systems require compliance with Section VIII, Process for Requesting New Credit Card Services and Equipment, A. Contract Language for Credit Card Payment Systems, of this document

B. Working Remotely

Staff involved with credit card functions working remotely are required to adhere, comply, and acknowledge all applicable policies and procedures. Proof of acknowledgement must be provided to the CFO's Finance Administrative & Compliance Services Division.

1. **Annual Training Courses:** Staff involved with the credit card processing functions must have taken the appropriate trainings, to include the PCI annual required online course and prior to working remotely have taken the annual refresher PCI course. Proof of completion must be provided to CFO.

2. **Attestation of Compliance Form:** Employees who work remotely will be required annually to sign an attestation acknowledging their responsibility in protecting and securing the credit card data from breaches or otherwise**.**

3. **Approved Miami-Dade Entity Equipment:** Staff may only use Miami-Dade Entity approved equipment, (i.e., laptop, cellphone, POS terminal and Mi-Fi) to process payments.

4. **Physical Control:** To safeguard home workspace the area should be securely maintained and inaccessible to unauthorized individuals. Employees should disable camera or recording functions when processing credit card transactions. Computer screens should be locked when leaving workspace area and all passwords secured.

5. **Point-of-Sale (POS) Device Inspections:** Supervisory Staff should periodically check devices for any skimmers; a log should be maintained of the review. Devices should be in a physically secure location when not in use. Employees who work remotely and are using POS devices must periodically check devices for skimmers and maintain a tampering log, which will be reviewed by the departmental PCI Liaison. Any suspected breaches should be reported immediately by completing

an on-line incident reporting form. *(Refer to Payment Device Inspection Log for instructions)*

6. **Workspace Area:** Employee may be asked to turn the camera function on, so the CFO's PCI Team can virtually review the devices serial number workspace area, if needed.

   Note: *Any materials or equipment taken home and/or to the approved designated remote work location must be kept in the designated work area and not be made accessible to others.*

7. PCI -DSS Protecting Payments While Working Remotely handout should be reviewed and acknowledged. Information on handout can be found at: https://blog.pcisecuritystandards.org/protecting-payments-while-working-remotely

8. The following training for PCI Liaisons is recommended. Information on the training can be found at: https://www.pcisecuritystandards.org/program_training_and_qualification/work_from_home_security_awareness

Refer to 334 – Clerk of the Court and Comptroller of Miami-Dade County Credit Card Processing Procedures for Working Remotely for further guidance.

V. Accounting Controls

A. Chargeback Processing

There are several mediums for receiving chargebacks, i.e., secured email, and/or secured portal.

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 securely cross shredded as soon as they are processed. If chargebacks are received via email, 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.
2. The vendor must be contacted and informed if full credit card numbers are visible in documents sent.
3. If the fax machine has a memory card, special care should be taken to clear the memory card from the fax machine daily.
4. Staff member issuing chargebacks may not also conduct regular sale transactions and/or have reconciliation/Deposits processing duties.
5. Only staff with a level of an Accountant 2 or above will be approved for chargeback access.
6. 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 Primary Account Number (PAN) is not visible, but only the last four (4) digits when 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/Deposits processing 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 Miami-Dade Entity with physical POS 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 (Deposits) used to record the transactions into INFORMS Accounts Receivable submodule and the location's description. Maintain copies for audit review.
3. The Deposits will be reviewed and approved by the department supervisor.

Any change or update as it relates to new staff handling chargebacks and refunds, a memo should be signed by the Miami-Dade Entity Director/Constitutional Officer, Deputy Director, or Delegated Authority. It must be submitted to the CFO's PCI Team advising of such change, if all else remains the same. Such changes will need to be reflected in the Miami-Dade Entity annual credit card procedures.

Note: Miami-Dade Entities will need to ensure that those employees who process chargebacks and refunds do not also process reconciliations. There must be a segregation of duties.

VI. Point-of-Sale (POS) Devices

POS Devices 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 once every month** 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.

Note: Periodic Tampering logs must also be maintained for all devices that accept credit card data, i.e., Pay on Foot (POF) terminals, TVMs, computers, P2PE terminals, and Kiosks, etc.

Wireless terminals that are not P2PE compliant 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. CFO's Cash Management Division must be contacted to order credit card equipment.**

Terminals may **NOT** be connected to the **MDC Network** unless these are pre-approved Point-to-Point Encryption (P2PE) devices. Miami-Dade Entities are not allowed to expand their payment process under any circumstance unless approved through the PCI Compliance Team (no payments can be taken outside the P2PE terminals). (Contact **CFO's** Cash Management Division or PCI team for additional information on P2PE services) and pricing. Broken terminals shall be reported to the **CFO's** Cash Management Division for replacement/disposition instructions.

VII. 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. Non-compliance to these standards can result in significant fines assessed to the Miami-Dade Entity and may result in loss of the ability to accept credit cards.

In order to ensure compliance with PCI DSS, Miami-Dade Entities that accept credit card payments must complete an annual PCI Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC). The PCI Team must conduct, quarterly vulnerability scans, and both an annual formal risk assessment, and penetration tests 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 PCI Team jointly monitor compliance and work with Miami-Dade Entities to provide training and information to comply with these requirements.

Build and Maintain a Secure Network
Requirement 1: Install and maintain Network Security Controls
Requirement 2: Apply Secure Configurations to All System Components.
Protect Account Data
Requirement 3: Protect Stored Account Data.
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program
Requirement 5: Protect All Systems and Networks from Malicious Software.
Requirement 6: Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures
Requirement 7: Restrict Access to System Components and Cardholder Data by

Business Need to Know.
Requirement 8: Identify Users and Authenticate Access to System Components.
Requirement 9: Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data.
Requirement 11: Test Security of Systems and Networks Regularly
Maintain an Information Security Policy
Requirement 12: Support Information Security with Organizational Policies and Programs.

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 Clerk's Payment Card Industry Executive Charter and Compliance Policy #332, as mentioned in section III.

A. Technical Requirements:

1. All service accounts, developer accounts and administrator accounts must use County Active Directory authentication. Any exceptions to this must be approved by the CITD Security office.
2. Details of encryption must be provided in the vendor's documentation and Diagrams (environment).
3. Passwords must be encrypted using a minimum of 256-bit encryption and must follow County password policy.
4. All remote access and non-console administrator access must use dual-factor authentication.
5. Submit a Security Review Remedy ticket for a Security Architecture review to ensure proper segmentation as well as access controls.
6. Ensure that the FireEye agent, File Integrity Monitoring on critical files and Microsoft System Center Configuration Manager (SCCM) are implemented and running.
7. All servers must send security logs to the Enterprise security system (currently Helix). You may contact CITD Enterprise Security Office for directions on this.

B. Security Approvals Required Before Go-Live:

1. Submit a security scan in Remedy system for any applications accessed via URL and obtain approval.
2. Submit a security scan in Remedy system for any servers being installed in the County network (that has an IP address) and obtain approval. Indicate the system is in PCI scope and a PCI scan is also required.

VIII. Process for Requesting New Credit Card Services and Equipment

Once the Miami-Dade Entity considers implementing a new system that includes payment capabilities, they need to contact the CFO's Administrative & Compliance Services Division to discuss the Scope of Work. The Contract Language for Credit Card Payment systems, along with steps found in Section B must be followed.

Note: *Currently, there is one main merchant processor that servicing departments and constitutional offices. In implementing a new system, Miami-Dade Entities are required to use the main merchant processor. In the event, the Miami-Dade Entity cannot use the main merchant processor based on the complexity of their business operations, they must submit the required documentation (memo, procedures, diagrams, MID/inventory, PCI certification, P2PE Pricing Sheet, if applicable) in addition to a Cost Benefit analysis to the CFO's Administrative & Compliance Services Division for review and determination.*

A. Contract Language for Credit Card Payment Systems

New payment systems going through the Request for Proposal (RFP) process must include the necessary language as stated below in Contract Language. Two members of the PCI Team must be part of the RFP process for any solicitations that involve systems with the capability to store, process, or transmit payment card data, and at least one shall be a voting member and the other shall be a technical advisor of the Selection Committee.

Note: *Requests for new credit card systems* ***cannot*** *be procured through Small Purchase Orders (SPOs) because of their recurring compliance requirements. Must consult with the PCI Team for guidance.*

The PCI Team will need to review the Scope of Work for any RFP that includes a payment system. This is applicable to all payment systems purchased non-competitively (Bid Waivers) including extensions of current contracts.

Once the contract has been awarded, the Miami-Dade Entity must forward the executed contractual agreement to the ***CFO's*** *Administrative & Compliance Services Division.*

Required Contract Language:

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, Non-Competitive contracts, and/or agreements and must be agreed by the selected vendor for the systems being procured/implemented.

The contractor shall comply with the Payment Card Industry Data Security Standards (PCI-DSS) in effect throughout the term of this Agreement. The contractor is responsible for ensuring that its systems, equipment, software, hardware, and policies remain PCI compliant at all times. If any component becomes non-compliant, the Contractor shall bear all costs necessary to restore compliance and complete it on a timely manner.

1. Proof of Compliance

The Contractor affirms knowledge of and commitment to PCI DSS compliance and shall provide the following documentation:

- A current annual PCI Compliance certification if applicable. The County reserves the right to audit this compliance and request copies of such certifications at any time.
- During installation or any major system upgrade, implementation manuals and detailed data flow diagram(s) must be submitted. These diagrams must illustrate all cardholder data flows across Miami-Dade County systems and networks, including the internet and the processor network.
- A completed Security Matrix for new systems - MDC IT Security Matrix - v112024.docx.
- The Contractor shall annually submit the updated, completed, and signed PCI compliance documentation demonstrating continued compliance to the County. annually to the County.

2. Ongoing Compliance and Updates

The Contractor Shall

- Update its solution as needed to maintain compliance with all changes to PCI standards and requirements in accordance with implementation dates mandated by the PCI Security Standards Council.
- Remediate any critical security vulnerability within thirty (30) days of identification.

3. Required Documentation in accordance with PCI requirement 12.9.2

Upon County request, the Contractor with third party payment solutions shall provide:

- PCI DSS compliance status information for services performed by the third-party contractor on behalf of the department in accordance with PCI Requirement 12.8.4.
- Documentation outlining responsibility of the contractor and responsibility of the county, including any shared responsibilities (e.g., Responsibility Matrix), in accordance with PCI Requirement 12.8.5.

4. Data Storage Restrictions

The Contractor agrees:

- Sensitive Authentication data and Primary Account number shall not be stored at any time, even in masked format.
- No cardholder data shall be stored unless absolutely necessary for the County's operations and explicitly approved by the County.

5. Point-of-Sale (POS) Compliance

- All POS devices must route transactions directly to the County's merchant provider.
- Devices must be EMV (Europay, Mastercard and Visa) compliant and capable of accepting Near Field Communications (NFC) payment methods, such as Google Wallet, Apple Pay, or Samsung Wallet.

6. Validation for Payment Processing Applications

For any payment processing application, the Contractor shall submit:

- A current Attestation of Compliance (AOC)
- A current Attestation of Validation (AOV), if applicable, countersigned by the PCI Security Standards Council.

7. Point-to-Point Encryption (P2PE) Requirements

- Cashiering Application systems that utilize the County network must implement a validated PCI P2PE solution, and transactions routed through the approved County merchant processor.
- The approved County's P2PE solution is Elavon's PCI Safe T P2PE Link Protect services.
- The Contractor shall provide confirmation of P2PE solution validation from PCI Council's official listing:

  https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions?agree=true

  Prior to the payment solution becoming operational and starts handling live credit card transactions the Contractor shall provide P2PE Instruction Manual (PIM). This manual is a standardized document, formatted in accordance with the PCI Security Standards Council guidelines:

  https://www.pcisecuritystandards.org/documents/P2PE_v3.0_PIM_Template.docx?agreement=true&time=1645920000555.

8. Internal Payment Gateway Use

- For systems and applications housed in County network, the payment transactions must be routed through Miami-Dade County's Internal Payment Gateway.

- Any exceptions to these requirements must be supported by a written justification from the Department Director **prior to** the purchase of software/hardware. This justification must include a cost/benefit analysis and must receive written approval from the County's Clerk of the Court and Comptroller – Comptroller Finance Operations Director.

- Transactions processed through the County Internal Payment Gateway are prohibited from accepting / processing PIN numbers for security reasons.

9. Payment Gateway Integration Options

The County provides the following two integration options for Contractor's application to interact with its Payment Gateways:

- Web-based Credit Card Transaction Service, and
- Recurring Payment Service – enables merchants to process recurring monthly or annual credit card payments on behalf of payers. This service operates via a PCI-compliant SOAP Web Service. The County will provide the WSDL and all required technical documentation. All sensitive credit card data is securely stored offsite in the County's clearinghouse.

To utilize these services, the Contractor may select from the following integration options based on the technical capabilities and hosting environments of their application:

9.1 Option 1. Direct Integration with the County's Payment Gateway

The Contractor's application interfaces directly with the County's Payment Gateway via a RESTful web-service. The County will provide:

- XML schemas to all basic services (web payment processing, void, refund, and recurring payments)
- All the necessary URLs for these services
- Technical documentation for data fields and response codes.
- Standard XML receipt format for all service responses.

This option offers maximum flexibility and customization but requires full development and integration effort by the Contractor. Additionally, the Contractor's application must be hosted within the County's managed network, as the Payment Gateway is not accessible from the internet.

If the Contractor's application is hosted outside of the County's managed network, Option# 2 must be used unless otherwise approved.

9.2 Option 2. Integration via County-Developed Payment Module Web Application

Under this approach, the Contractor will integrate with a County-developed Payment Module Web Application, which may be used as a standard or mobile we app. Key integration features include:

- A "Pay Now" button within the Contractor's application redirects payers via secure HTTPS POST to the County's Payment Module, passing necessary data (E.G., User ID, amount).
- The Contractor and County will agree on any custom fields transmitted over TLS 1.2 or higher (SSL is not accepted).
- The County's Payment Module collects payment information and processes the transaction using the County's Internal Payment Gateway.
- Upon completion, the results are posted back to the Contractor's application via a client-specified return URL.

This solution requires minimal development effort from the Contractor and does not require hosting within the County's managed network. The County assume responsibility for all processing logic and system error handling.

9.3 Option 3. Independently Validated PCI-Compliant Solution

If the Contractor cannot use Options 1 or 2 and must operate independently of the County's Payment Gateway, the Contractor may propose an external PCI-compliant solution, provided it:

- Is fully compliant with the latest PCI DSS version
- Includes independent validation of compliance by a Qualified Security Assessor (QSA).

Required documentation includes:

- Attestation of Compliance (AOC)
- Detailed technical architecture, including data flow diagrams showing all cardholder data interactions
- A comprehensive description of all security measures in place (by the Contractor and any subcontractors)

The proposed solution will be subject to review and approval by the County's PCI Committee, followed by final authorization by County Senior Management. The requesting County Department must submit a formal memorandum and cost-benefit analysis in support of the solution.

As part of this option, the Contractor and subcontractors must:

- Ensure secure transmission and storage of cardholder data
- Undergo periodic PCI compliance audits
- Provide ongoing assurance of PCI DSS adherence for the duration of the agreement.

B. Required Documentation for Requesting Credit Card Services and Equipment. When requesting approval for implementing new credit card services, Miami-Dade Entities shall fully explain the type of service, application, and procedures that will be implemented **prior to procurement/development**. The following are required:

I. Memorandum from the Miami-Dade Entity Director/Constitutional Officer,

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

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

IV. Merchant Identification Report (MID Report),

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

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

VII. A completed copy of the Miami-Dade County Security Matrix, if using a third-party vendor. MDC IT Security Matrix - v112024.docx

VIII. Roles and Responsibility *(Shared Responsibility Matrix),*

IX. All cloud service providers must provide access to review the SOC 1 and SOC 2 (Service Organization Control 1 & 2) report.

X. Cost Benefit Analysis/P2PE Pricing Sheet (if using non-Elavon P2PE solution)

a. To include the Miami-Dade Entity Director/Constitutional Officer or Delegated Authority and CFO Director signatures.

XI. P2PE Instruction Manual (If using P2PE solution)

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. Include what type of process the request is for.

2. Describe the channels used to process transactions (in person, e-commerce, and telephone) List the channel payments are transacted through (Web, POS, P2PE, Pay on Foot, Kiosks, TVMs, County Payment Gateway, Third Party Vendor Software, Hosted Payment Page, etc.) (and if the transactions will be processed through the County's Gateway or directly to payment processor, Elavon. **Note:** *COCC's Policy is to have all credit card transactions processed via the County Gateway unless an exception is approved by the CFO Director or Director's designee.* All third-party payment systems shall be PCI compliant. Miami-Dade Entities selecting P2PE services must complete P2PE Pricing Sheet available through CFO's Cash Management Division. Both the CFO's Administrative & Compliance Services Division and County CITD 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 VIII. (A), *"Contract Language for Credit Card Payment Systems."*

3. Describe why the Miami-Dade Entity is transitioning from current system to new solution. Include the benefits associated with the transition.
4. Any cost saving benefits if using a non-County approved vendor.
5. If not using the County approved vendor, include the cost benefit pricing worksheet.
6. 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 Clerk of the Court and Comptroller Payment Card Industry Executive Charter and Compliance Policy #332 and Credit Card Acceptance and Processing Procedures #333.
7. 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.
8. Include request for new equipment (Point-of-Sale Devices), who will be the contact and where they will be shipped.
9. Include a tentative Go-Live Date. Go Live dates between April and June are discouraged as this is the audit period.
10. Memorandum should be signed and approved by the respective Miami-Dade Entity Director/Constitutional Officer.

II. **Credit Card Procedures -** Follow the guidelines established in these procedures and use the approved template (refer to section XI.).

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 provided by the CFO's Administrative & Compliance Services Division and must be reviewed and updated every six months or when requesting a new payment process.

V. **PCI Scope Inventory Report** – Provide an inventory report of all the hardware that will be used in the credit card environment. The Enterprise Security Office at CITD can be contacted for assistance with this report. The report can be provided by the CITD Enterprise Security Office. It must be reviewed and updated every six months or when there is a change in the credit card environment.

VI. **PCI certification –** Miami-Dade Entities must retain vendor PCI related documentation for third-party payment services, i.e., Software Security Framework (SSF), Attestation of Compliance (AOC), Attestation of Validation (AOV), PCI P2PE validation found in the PCI website and/or the P2PE Instruction Manual (PIM).

All required documents shall be submitted to the CFO Director by submission through the Administrative & Compliance Services Division (FIN-Compliance@miamidade.gov) for review and approval.

Any change in the credit environment (payment processor, server etc.) must go through the PCI Team prior to implementing.

Approval process:

1. A review of the documents will be completed by the PCI Team to ensure compliance with the respective procedures and PCI guidelines. If all is acceptable, the CFO Director or designee will approve the request, and the merchant and user forms will be provided by CFO's Cash Management Division and sent to the respective PCI Liaison for processing.

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

3. Setup forms are signed by the requesting Miami-Dade Entity Director/Elected Officer, or designee, and the CFO's Director or designee, approving the set-up of both the merchant account (with the merchant processing company) and the Gateway account (with CITD). Please note, CITD will not setup new accounts and/or new users unless signed set up forms are received.

4. CFO's 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. CFO's Cash Management Division forwards the form to the Miami-Dade Entity 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 Miami-Dade Entity fills in all necessary information (except bank information) and returns the form (via email) to CFO's Cash Management Division, who will fill in the bank information and forward to the processor company.

6. Miami-Dade Entity PCI Liaisons should send an email to CFO's 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/CO name.
   d) Shipping address.
   e) Attention to; and
   f) Include if needed, a request for Call Tags to be sent to the Miami-Dade Entity. Call Tags are used to return broken, outdated, etc., equipment back to the merchant processing company for proper disposal.

7. The processor notifies the CFO's Cash Management Division when the account is opened. Cash Management Division will, in turn, notify the Miami-Dade Entity 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.

   Note: For an additional MID request, modification of MID name, or to cancel a MID, a memo acknowledging the business justification should be submitted by the Miami-Dade Entity and signed by the Director/Constitutional Officer or Delegated Authority.

8. CFO's Cash Management Division will coordinate with the Miami-Dade Entity and the merchant processor to evaluate various factors that may affect the service, such as dollar volume, average ticket size, etc.

9. The Miami-Dade Entity should contact the CFO's Bank Reconciliation Unit FIN-BR@miamidade.gov for information on Deposits, reports, etc., that may be needed for reconciliation purposes.

IX. PCI Liaison

The PCI Liaison will be responsible for monitoring PCI compliance within their respective Miami-Dade Entity, reviewing entity documentation once every six months or when there is a change, 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. Miami-Dade Entity procedures, PCI scope inventory, merchant identification report, diagrams, third party payment application certifications will need to be reviewed/updated every six months. In addition, the liaison will need to work with CFO and CITD to coordinate and ensure timely preparation, review, and approval of the Self Attestation Questionnaires (SAQs) and Attestation of Compliance (AOC) forms (which must be submitted through secured email).

The PCI Liaison is also responsible for ensuring that there are no changes in the credit card environment as noted in the most recent certifications (policies procedures, PCI Scope Inventory reports/MID's) taken place without the appropriate approval beforehand.

Detail of Miami-Dade County Entities and PCI Liaisons responsibilities can be found in the Clerk of the Court and Comptroller Payment Card Industry Executive Charter and Compliance Policy 332, section VII, (A and B).

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

X. Approvals

Request for new credit card services will require a memorandum approved by the Miami-Dade Entity Director/Constitutional Officer (refer to section VIII, (B)(I), "*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 Miami-Dade Entity's PCI Liaison and the Director/Constitutional Officer.

It is the Miami-Dade Entity's 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 Clerk of the Court and Comptroller Payment Card Industry Executive Charter and Compliance Policy #332.

Any change or updates to be made during the year, to your current process (i.e. PCI Liaison updates, chargebacks processes, reconciliation processes etc.), a memorandum is required acknowledging the change and include that all other information remains the same to be signed by the Miami-Dade Entity Director/Constitutional Officer, Assistant/Deputy Director and/or Delegated Authority. These changes or updates must also be included in the Miami-Dade Entity's annual submission of documentation for the PCI annual assessment.

If there are any changes or updates to the credit card environment (i.e. new payment application, processor, payment channels, etc.) the Miami-Dade Entity will need to refer to section for Section VIII, (B). *Required Documentation for Requesting Credit Card Services and Equipment*.

XI. Template for requesting new and updated services:

Miami-Dade Entity (Insert Department/Constitutional Office 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 business needs identified to justify the need for accepting credit cards.

2. Channels used to process transactions (in person, e-commerce, and telephone). List the channel payments are transacted through (Web, POS, P2PE, Pay-on-Foot, Kiosks, TVMs, County Gateway, Third Party Vendor Software, Hosted Payment Page, etc.) Note: COCC's Policy is to have all credit card transactions processed via the County's Payment Gateway unless an exception is approved by the Comptroller Finance Operations (CFO) 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 through 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 channels (including reports used, processing cutoff times, titles of responsible staff, etc.). State that protecting credit card information 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) or writing credit card information, which should be entered directly to the system or Point-of-Sale (POS) terminal as it is received from the customer *(Note: for P2PE terminals, credit card information should be entered directly into the terminal itself, not the cashiering system).* 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, and staff that is processing payments will not have access to their personal devices while completing the transaction.

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, 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 the system or POS terminal, 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. If working from home, refer to Section IV (B). for additional instructions.

4. Via Fax or Email: **Credit card information must 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/cross shredded, 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 CITD, and confirm that no Cardholder information is saved/stored at the location. Include the URL link where internet payments are processed through as well as who is responsible for the compliance of the webpage.

6. Pay On Foot (POF) / Kiosks/TVMs: Explain if this method is being used to process payments. Also, confirm if the area is secure (security cameras etc.).

III. Chargeback processing:

1. There are several mediums for receiving chargebacks, i.e., secured email, and/or portal. 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 email, it must be received through a secured access and only the last four digits of the credit card number should be visible for processing. Include the name and title of the staff members receiving the chargeback email notifications.

2. 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 secured email and there is credit card information received, explain that the information will be immediately deleted.

3. Confirm that the staff member issuing chargebacks does not also conduct regular sale transactions and/or have reconciliation/Deposits processing duties.

4. 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.

   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:

1. 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 visible, but only the last four (4) digits when received from the credit card provider. Explain if at any moment full PAN is visible when received, the information should be securely cross-shredded.

   Note: In the event it becomes necessary for an employee(s) in this role to view the full PAN, the Miami-Dade Entity must first advise the CFO's Administrative & Compliance Services Division with justification of the business need, describe the controls in place to secure the information and confirm PCI training has been completed. Those employees will also be required to sign an Attestation of Compliance which will be provided.
2. Confirm that the staff member issuing refunds does not also conduct regular sale transactions and/or have reconciliation/Deposits processing duties.
3. 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.
4. Supervisors must review and approve each refund; the name and title of those supervisors will need to be provided and updated annually.
5. 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:

1. POS Terminals shall be closed out each day with a batch settlement process.
2. A detailed reconciliation process shall be done at least monthly, which shall include reports (Deposits) used to record the transactions into INFORMS Accounts Receivable submodule and the location's description. Maintain copies for audit review.
3. The Deposits will be reviewed and approved by the department supervisor.

VI. Terminals:

1. 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.
2. Confirm that a unique PIN will be used by each staff member using the terminal and that staff understands that PINs cannot be shared.
3. Confirm that there is a documented and a periodic inspection process in place at least once a month to detect for any tampering of equipment (unauthorized payment card skimmers) and that a log is maintained. The log must also include any devices accepting payment card data, i.e., POF devices, computers, P2PE terminals, TVMs, and kiosks etc. *(Refer to Payment Device Inspection Log for instructions)*
4. Provide the physically secure location where terminal will be stored when not in use.
5. Confirm that terminals will not be connected to the network.
6. If using a wireless terminal, confirm the cellular carrier being used and that it has been approved through the County's approved processor.
7. Confirm that CFO's Cash Management Division will be contacted for instruction on disposition/replacement of all terminals.

VII. PCI Liaison:

On a yearly basis, the Miami-Dade Entity will need to complete and sign (by the Miami-Dade Entity Director/Constitutional Officer) a Self-Assessment Questionnaire (SAQ) or Report on Compliance, and Attestation of Compliance (AOC) form, as mandated by the Payment Card Industry Data Security Standard (PCI DSS). The Procedures should also contain the following:

1. The Name and title of the PCI Liaison to oversee the credit card processing and work with CFO and CITD on PCI compliance and training.
2. Include a statement that this policy will be reviewed/updated upon changes to the credit card environment and/or annually.
3. Include a statement that all staff involved with the credit card processing functions will be trained and provided with a copy of Clerk's 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 CFO and approved by the respective Miami-Dade Entity Director/Constitutional Officer.

Summary of documents for submission to CFO:

1. Memorandum from the Miami-Dade Entity Director/Constitutional Officer
2. Credit Card Procedures
3. Diagram(s) (environment)
4. Merchant Identification Report (MID Report)
5. PCI Scope Inventory Report (hardware, software)
6. PCI Certification (if using a third-party vendor application)
7. A completed copy of the Miami-Dade County Security Matrix, if using a third-party vendor.
8. Roles and Responsibility (Shared Responsibility Matrix)
9. All cloud service providers SOC 1 and SOC 2 (Service Organization Control 1 & 2) Report access/review
10. Cost Benefit Analysis/P2PE Pricing Sheet (if using Non-County Elavon P2PE solution)
11. P2PE Instruction Manual (If using P2PE solution)

Note: *Annual update requires submission of items above and upon any change in the credit card process.*

Approvals: The procedures must be signed/approved at least by the Miami-Dade Entity's PCI Liaison and the Director/Elected Officer.

By approving below, we acknowledge that the (Insert Name of Miami-Dade Entity) personnel involved with credit card processing as stated in this policy, have read, and will comply with the Clerk of the Court and Comptroller of Miami-Dade County Payment Card Industry Executive Charter and Compliance Policy #332 and the Credit Card Acceptance and Processing Procedures #333.

Miami-Dade Entity PCI Liaison	Date
Miami-Dade Entity Director/Constitutional Officer	Date