## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

## INTRODUCTION

The purpose of these procedures is to provide guidance for accepting credit card payments for services throughout Miami Dade County (County). 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

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

## I. Revisions to Procedure:

This section documents the revisions made to this procedure since the last approved version dated November 2021.

| Effective Date | Version | Description | Pages |
|---|---|---|---|
| October 2019 | 333.1.0 | General grammatical changes | |
| January 2021 | 333.2.0 | Added Scope and Applicable Policies and Procedures | 2 |
| January 2021 | 333.2.0 | Working Remotely Process | 5 |
| January 2021 | 333.2.0 | Added requirements and weblinks for P2PE | 10 |
| January 2021 | 333.2.0 | Added verbiage to internet transactions and exceptions in section VIII | 11 |
| January 2021 | 333.2.0 | Technical requirements and general grammatical changes | 3,4,5,8, 9, 15, 17, 19, 20 |
| November 2021 | 333.3.0 | Clarified abbreviations | 3, 5,10 |
| November 2021 | 333.3.0 | Verbiage for new services updated | 4 |
| November 2021 | 333.3.0 | Included PCI links for Working Remotely handout and Training | 6 |
| November 2021 | 333.3.0 | Updated Refund and Reconciliation section to reflect new Informs process | 7,8,21,22 |
| November 2021 | 333.3.0 | Updated verbiage for exceptions | 11 |
| November 2021 | 333.3.0 | Location of MID/Inventory Report and submittal of new payment request | 18 |
| November 2021 | 333.3.0 | Bank reconciliation information for deposits | 19 |
| November 2021 | 333.3.0 | Approval statement updated | 23 |
| November 2021 | 333.3.0 | General grammatical changes | 2,3,4,5,6,7,8,9,10,17,18,19,20,21,22 |

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

| August 2022 | 333.4.0 | Added links and revised name | 4 |
|---|---|---|---|
| August 2022 | 333.4.0 | General Grammatical changes | 4,5,7,8,11,12,13,16,18,21,22,24 |
| August 2022 | 333.4.0 | Working Remotely section added Attestation of Compliance document and Workspace Area | 7 |
| August 2022 | 333.4.0 | Added verbiage | 7,9, 0,12,13,14,17,18,20 |
| August 2022 | 333.4.0 | Moved section and added language for SOC2 and Security Matrix | 16 |
| August 2022 | 333.4.0 | Added language for SSF Framework | 17 |
| August 2022 | 333.4.0 | Moved Required Documentation Section and Template Section | 16,19, 20 |
| August 2023 | 333.4.0 | Added verbiage and reworded to include the listing of payment channels and methods payments are transacted through | 17,22 |
| August 2023 | 333.4.0 | Added the Security Matrix link to be used when requesting new payment application | 14,17 |
| August 2023 | 333.4.0 | Updated the Division name | 6,12,13,18,19 |
| August 2023 | 333.4.0 | Added verbiage and additional credit card handling payment channel | 23 |
| August 2023 | 333.4.0 | Added verbiage regarding tampering | 10, 25 |
| August 2023 | 333.4.0 | Added verbiage for additional controls in place | 24 |
| August 2023 | 333.4.0 | Added verbiage regarding Contract language for process for small PO | 13 |
| August 2023 | 333.4.0 | Updated Security Matrix link | 17 |
| August 2023 | 333.4.0 | Removed verbiage regarding vendor form | 13 |

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

### II. Scope:

All County employees involved in processing credit card transactions and in the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) are subject to 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/333.pdf

- Miami Dade County Enterprise Information Security Policy Manual
  http://intra.miamidade.gov/technology/library/guidelines/security-policy-manual.pdf

- Payment Card Industry Data Security Standards Incident Response Plan
  http://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf

- Miami Dade County Identity Theft Prevention Program (Red Flags-Resolution R-580-10
  http://www.miamidade.gov/govaction/legistarfiles/Matters/Y2010/101045.pdf

- Miami Dade County Credit Card Processing Procedures for Working Remotely (Procedure #334)
  https://intra.miamidade.gov/finance/payment-card-industry.asp

### IV. 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.

New services will be requested through the Finance Department 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 departmental 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

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

Departments must use the credit card payment processor(s) under contract with the County. The Finance Cash Management Division and the Administrative & Compliance Services 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 in addition to mandatory on-line training courses that each department is responsible for ensuring their respective employees complete. Refer to Policy #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.

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 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. Ensure that conversation(s) 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. (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, 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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

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 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.

5. **Internet:** Transactions shall be processed via the County's Gateway managed by the Information Technology Department (ITD) and no cardholder information shall be saved/stored. Third Party payment application systems require compliance with the section VIII, "Contract Language for Credit Card Payment Systems".

### 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 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 on-line course and prior to working remotely have taken the annual refresher PCI course. Proof of completion must be provided to the Finance Department.

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 County Equipment:** Staff may only use County approved equipment, (i.e., laptop, cellphone, POS terminals and Mi-Fi) to process payments.

4. **Physical Control:** To safeguard home workspace the area should be securely maintained and inaccessible to unauthorized individuals.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

Employees should disable camera or recording functions when processing credit card transactions. Computer screens and should be locked when leaving workspace area and all passwords secured.

5. **Terminal Inspections:** Supervisory Staff should periodically check POS terminals for any skimmers; a log should be maintained of the review. POS terminals 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.

6. **Workspace Area:** Employee may be asked to turn the camera function on, so the PCI Compliance 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 - Miami Dade County Credit Card Processing Procedures for Working Remotely for further guidance.*

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

### V. Accounting Controls

#### A. Chargeback Processing:

1. There are several mediums for receiving chargebacks, i.e., fax, email, 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 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. 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/Deposits processing 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/Deposits processing duties. 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).

**CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES**

### 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 (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.

*Note: Departments 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. 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.

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

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 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. Departments 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 Finance Cash Management Division or PCI Compliance team for additional information on P2PE services) and pricing. Broken terminals shall be

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

reported to the Finance 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. 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 (SAQ) and Attestation of Compliance (AOC). The County 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 County's PCI Compliance Team 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, as mentioned in section III.

| |
|---|
| **Build and Maintain a Secure Network** |
| Requirement 1: Install and maintain a firewall configuration to protect cardholder data. |
| Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. |
| |
| **Protect Cardholder Data** |
| Requirement 3: Protect stored cardholder data. |
| Requirement 4: Encrypt transmission of cardholder data across open, public networks. |
| |
| **Maintain a Vulnerability Management Program** |
| Requirement 5: Use and regularly update anti-virus software or programs. |
| Requirement 6: Develop and maintain secure systems and applications. |
| |
| **Implement Strong Access Control Measures** |
| Requirement 7: Restrict access to cardholder data by business need to know. |
| Requirement 8: Assign a unique ID to each person with computer access. |
| Requirement 9: Restrict physical access to cardholder data. |
| |
| **Regularly Monitor and Test Networks** |
| Requirement 10: Track and monitor all access to network resources and cardholder data. |
| Requirement 11: Regularly test security systems and processes. |
| |

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

| Maintain an Information Security Policy |
| --- |
| Requirement 12: Maintain a policy that addresses information security for all personnel. |

### A. Technical Requirements:

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

### Security Approvals required before Go-Live:

- Submit a security scan in Remedy system for any applications accessed via URL and obtain approval.
- 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 department considers implementing a new system that includes payment capabilities, they need to contact the Finance 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: In implementing a new system, Elavon, Inc. is Miami Dade County's approved payment processor and departments are required to use Elavon as the merchant processor. In the event, the department cannot use Elavon based on the complexity of their business operations, they must submit the required*

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

*documentation (memo, procedures, diagrams, MID/inventory, PCI certification, P2PE Pricing Sheet, if applicable) in addition to a Cost Benefit analysis to the Finance 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 County's PCI Team must be part of the RFP process for any solicitations that involve systems with the capability to process payments, and at least one shall be a voting member.

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

*The County's PCI Team will need to review the Scope of Work for any RFP that includes a payment system.*

*Note: Once the contract has been awarded, the Department must forward the Contract Number to the Finance 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, 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, the 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

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

data flows across MDC's systems and networks, the internet, and the processor network.

3. Provide Security Matrix for new systems - IT Security Matrix - ESO Updated 01262023.docx

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) must be routed directly to Miami-Dade County's merchant provider (ELAVON) and must be EMV compliant. All POS devices must be capable of accepting NFC (near field communications) payment methods such as Google Wallet, Apple Pay, or Samsung Wallet.

e. For payment processing applications, proof of validation must be countersigned by the PCI Council. Documentation to be submitted is as follows:

a. AOC for the application - Attestation of Compliance

b. Most current AOV - Attestation of Validation (when applicable)

f. Cashiering Application 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. The County's approved P2PE solution is Elavon's PCI Safe T P2PE Link Protect services. Confirmation of validated P2PE solution shall be provided as found on the PCI Council's P2PE Solutions website.

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

Prior to production going live, the P2PE Instruction Manual shall be provided as found on PCI website.

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

g. Internet transactions and all other applications must be routed through Miami-Dade County's Internal Payment Gateway (Payment Card).

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

h. Exceptions to any of these requirements shall require written justification by the Department Director **prior to** purchase of software/hardware, including a cost/benefit analysis, and require written approval by both the Miami Dade County Finance Director.

i. Transactions processed through the Miami-Dade County Internal Payment Gateway are prohibited from accepting / processing PIN numbers for security reasons. Miami-Dade County provides two basic services that allow Contractor applications to interact with its Payment Gateways:

   1. Web-based Credit Card Transaction Service

   2. 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 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 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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

### B. Required Documentation for Requesting Credit Card Services and Equipment.

When requesting approval for implementing new credit card services, departments 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 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)*

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

              IT Security Matrix - ESO Updated 01262023.docx

VIII.   All cloud service providers must provide a copy of the SOC 2 (Service Organization Control 2) report.

  IX.   Cost Benefit Analysis/P2PE Pricing Sheet (if using P2PE solution)
       a)   To include the Department Director and Chief Financial Officer signature

   X.   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 method used to process transactions (in person, e-commerce, telephone, Pay on Foot, Kiosks, etc.) List the methods payments are transacted through (Web, POS, P2PE, County 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. <u>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.</u> All third-party payment systems shall be PCI compliant. Departments selecting P2PE

services must complete P2PE Pricing Sheet available through Finance Cash Management Division. Both the Finance Administrative & Compliance Services Division 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 VIII. (a), "Contract Language for Credit Card Payment Systems."

3. Describe why the department is transitioning from current system to new solution. Include the benefits for the department 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 Miami Dade County 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 (terminal-Point of sale machines), 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 Department Director.

II. **Credit Card Procedures -** Follow the guidelines established in these procedures and use the approved template (refer to section XI. 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 provided by the Finance Administrative & Compliance Services Division and must be updated annually or when requesting a new payment process.

# CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

**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 provided by the ITD Security Office and must be updated annually or when there is a change.

**VI.** **PCI certification –** Departments 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 Finance 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 County's PCI Team prior to implementing.

*Approval process:*

1. A review of the documents will be completed by the County's PCI Team to ensure compliance with the 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 provided by Finance Cash Management Division and 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 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 the Finance Director or designee, 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

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

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 Deposits, reports, etc., that may be needed for reconciliation purposes.


## IX. PCI Liaison

The liaison will be responsible for monitoring departmental PCI Compliance, reviewing, and updating departmental documentation annually or when there is a change, and ensuring that appropriate staff is trained. All staff involved with the

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

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, the 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 (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, Inventory reports/MID's) taken place without the appropriate approval beforehand.

Detail of Department and PCI Liaisons responsibilities can be found in Miami Dade County 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 Department Director (refer to section XI., "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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

### XI. 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 business needs identified to justify the need for accepting credit cards.

2. Method used to process transactions (in person, e-commerce, telephone, Pay on Foot (POF) Kiosks, etc.). List the methods payments are transacted through (Web, POS, P2PE, County Gateway, Third Party Vendor Software, Hosted Payment Page, 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 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 methods (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) and writing credit card information, which should be entered directly to the system or 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

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

(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. <u>Via U.S. Mail:</u> **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. <u>In-person</u>: 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. <u>Via Fax or Email:</u> **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. <u>Internet:</u> 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. 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: Explain if this method is being used to process payments. Also, confirm if the area is secure (security cameras etc.).

### III. Chargeback processing:

a. There are several mediums for receiving chargebacks, i.e., fax, email, 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 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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

    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/Deposits processing 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. Note* in the event it becomes necessary for an employee(s) in this role to view the full PAN, the department must first advise the Finance 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.

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

    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.

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

b. 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.

c. The Deposits will be reviewed and approved by the department supervisor.

**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. The log must also include any devices accepting payment card data, i.e., POF devices, computers, P2PE terminals, and kiosks etc.

d. Provide the 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).

## CREDIT CARD ACCEPTANCE AND PROCESSING PROCEDURES

Annual certification of training completion must be submitted to the Finance Department and approved by the respective department Director.

**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, except #1.*

**Approvals:** The procedures must be signed/approved at least by the Department's PCI Liaison and the Department Director.

*By approving below, we acknowledge that the department personnel involved with credit card processing as stated in this policy, have read, and will comply with the MDC Payment Card Industry Executive Charter and Compliance Policy #332 and the Credit Card Acceptance and Processing Procedures #333.*

| | |
|---|---|
| Department PCI Liaison | Date |

| | |
|---|---|
| Department Director | Date |