Payment Card Industry
Executive Charter and Compliance Policy 332

Prepared By:

Miami-Dade County PCI Committee

Updated: *October 2024*

Revisions to Policy:

This section documents the revisions made to this policy since the last approved version dated November 2023.

Effective Date	Version	Description	Pages
October 2024	332.6.0	Updated department name	3
October 2024	332.6.0	Inclusion of Constitutional Office wording	4
October 2024	332.6.0	Updated PCI Council weblink	3
October 2024	332.6.0	General grammatical changes	
October 2024	332.6.0	Updated annual credit card transaction/sales volume	3
October 2024	332.6.0	Added new terms in Definition Section	5
October 2024	332.6.0	Updated PCI Six Goals verbiage	9
October 2024	332.6.0	Updated Training Requirements	10
October 2024	332.6.0	PCI Liaison Assignment – level of position	10
October 2024	332.6.0	Added/updated additional bullets in Roles & Responsibilities	11, 12, 13, 14, 15, 16
October 2024	332.6.0	Clarification on PCI Members in Selection Committee	14
October 2024	332.6.0	Added/updated verbiage	5, 8, 11, 12, 13, 14
October 2024	332.6.0	Updated Incident Response Plan weblink	18
October 2024	332.6.0	New/Updated PCI Project Calendar Items	20 through 36

Table of Contents

I. Purpose

The purpose of this policy is to assist in mitigating the risk of credit card fraud, hacking, and various other security vulnerabilities and threats, and to reduce the risk of a breach of cardholder data by adhering to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed by the founding members, comprised of American Express, MasterCard Worldwide, Visa Inc. Discover Financial Services, and JCB International, of the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC is responsible for managing and updating the security standards while compliance is enforced by the individual payment card brands. This policy will provide strategic direction and support to Miami-Dade County's (MDC) departments/elected offices processing credit card transactions as required by PCI DSS Req.#12.4.1 found in PCI Council document library: https://www.pcisecuritystandards.org/document_library/

II. Overview

MDC processes more than ten million transactions annually accounting for over $869 million dollars in credit card payments. There are twenty-six (26) departments/elected offices in MDC that process credit card payments at over 200 locations using a variety of payment channels, including but not limited to, Point of Sale (POS) devices, in-house developed applications, third-party payment applications, phone, and in-person. There are four (4) merchant processors servicing departments/elected offices.

Annually, each Miami-Dade County Entity (Department/Elected Office) is required to complete and update its credit card procedures explaining how transactions are processed in their respective department. These procedures shall be approved and signed by the department's PCI Liaison and the department's executive management (Department Directors). The updates include credit card procedures, Merchant ID (MID) report, the vendor's PCI compliance certification, technical diagrams, and inventory reports. The approved procedures along with the additional documentation are submitted to the Finance department by the respective department's PCI Liaison and posted to the County's PCI Team secured shared drive. The Finance Administrative & Compliance Services Division will review procedures and MID reports to ensure compliance with County's Policy and PCI requirements. The Information Technology Department Security Division (ITD) reviews PCI certification, technical diagrams, and inventory reports for compliance with PCI, technical, and security policies/procedures.

New department requests to process credit card transactions or changes in current processes require resubmittal of procedures to be approved prior to procurement and/or development. A review for internal controls and compliance with the Payment Card Industry Data Security Standards (PCI-DSS) is completed and reviewed for approval by the County's PCI Team. 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.

ITD conducts monthly internal scans based on inventory reports as provided by each of the departments and regularly checks the network and processes for any vulnerabilities. A quarterly scan result for the external facing devices is submitted to County processor(s). Annual internal and external penetration tests, bi-annual PCI segmentation tests, application penetration test, and targeted risk assessment are completed to identify any threats and/or vulnerabilities requiring remediation. Quarterly field visits are conducted by the Finance Administrative & Compliance Services Division to monitor and assist each Miami-Dade County Entity with PCI compliance.

III. Definitions

Acquirer – Also referred to as "acquiring bank" or "acquiring financial institution". Entity that initiates and maintains relationships with merchants for acceptance of payment cards.

AOC - Acronym for "Attestation of Compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.

AOV - Acronym for "Attestation of Validation." The AOV is a form for SSF Assessor to attest to the results of a Secure Software assessment, as documented in the SSF Report on Validation.

ASV – "Approved Scanning Vendor" - vendor who provides security and compliance services. For PCI compliance we are required to do a Quarterly external vulnerability scan using the services of an ASV and achieve a "PASS".

BIN – Acronym for "Bank Identification Number". The first six digits (or more) of a payment card number that identifies the financial institution that issued the payment card to the cardholder.

Cardholder – Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder data - any personally-identifiable data associated with a cardholder. Examples include, but are not limited to account number, expiration date, card type, name, address, and card validation code – the three or four-digit value printed on the front or back of a payment card referred to as CAV, CVC, CVV, or CSC depending on the payment card brand. The term cardholder data is interchangeable with payment card data throughout this policy.

Card Skimmer - A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.

Masking - In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See "Truncation" (definition below) for protection of PAN when stored in files, databases, etc.

Merchant – A department approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.

Miami-Dade County Entity – A county department or elected office that accepts credit card as payment.
Merchant Identification Number – A unique number that identifies the department approved to accept payment cards.

P2PE (Point to Point Encryption) – is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe, insert, tap, dip or manual entry) until the data reaches the solution providers' secure decryption environment.

Payment Card – Any credit, debit, or private label card accepted as a form of payment for goods and/or services or receipt of donations.

Payment Card Application – Any hardware, software, or combination of hardware and software that aid in the processing, transmitting, or storing of cardholder data as part of authorization or settlement. Examples include point of sale (POS) devices, ecommerce shopping carts, web-based payment applications, and third party (vendor) provided systems.

PCI - Acronym for "Payment Card Industry."

SSF-SA - Acronym for "Secure Software Framework Assessor." SSF-QAs are qualified by PCI SSC to assess payment applications against the SSF.

Payment Card Industry Data Security Standard (PCI DSS) – PCI DSS is a worldwide information security standard assembled by the Payment Card

Industry Security Standards Council (PCI SSC). The standard applies to all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The standard is maintained by the PCI SSC, which maintains both the PCI DSS and a number of other standards, such as the Payment Card Industry PIN Entry Device security requirements (PCI PED) and the PCI Software Security Framework (SSF) . The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The PCI DSS may be accessed at: https://www.pcisecuritystandards.org/.

Payment Card Industry Data Security Standard Self-Assessment Questionnaire (PCI DSS SAQ) – The PCI DSS SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple versions of the PCI DSS SAQ to meet various scenarios. Each unique version of the PCI DSS SAQ includes a Self-Assessment Questionnaire and Attestation of Compliance that must be completed annually by the merchant and/or service provider as appropriate.

Payment Card Processing – The processing, transmitting, and/or storing of cardholder data, i.e., acceptance of credit or debit cards.

Primary Account Number (PAN) – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “Account Number”.
QSA - Acronym for “Qualified Security Assessor.” QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.

ROC - Acronym for “Report on Compliance.” Report documenting detailed results from an entity’s PCI DSS assessment.

SAQ - Acronym for “Self-Assessment Questionnaire.” See “Payment Card Industry Data Security Standard Self-Assessment Questionnaire” (definition above) reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.

PCI SSF: Acronym for “Software Security Framework.” A collection of software security standards that leverage a common validation and certification model.

Truncation - Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See “Masking” (definition above) for protection of PAN when displayed on screens, paper receipts, etc.

IV. Accountability

Miami-Dade County Entities processing credit card transactions are required to adhere and comply with all applicable policies and procedures. Department Directors have full oversight over their respective departments and provide appropriate departmental approvals including those of the Self-Assessment Questionnaire (SAQ), Report on Compliance (ROC), and the Attestation of Compliance (AOC). The COCC Finance department reviews and monitors departmental PCI compliance and applicable policies and procedures. County ITD reviews and monitors departmental PCI compliance and compliance with technology related guidelines/regulations. The Finance Director approves the countywide SAQ/ROC and AOC that is submitted to the merchant processors. The elected Constitutional Officer/Delegate will approve SAQ/ROC and AOC for their respective office effective January 7, 2025.

The objectives of this policy are to ensure compliance with the PCI DSS and other applicable policies and standards, establish the governance structure for payment card processing and compliance activities, define responsibilities for payment card services, and provide general guidelines regarding the handling of cardholder data.

V. Applicability

This policy applies to all personnel responsible for processing, reviewing, reconciling, approving credit transactions or processes, and/or developing credit card applications. This policy also applies to any department who contracts with a third-party vendor to handle and/or process cardholder data on behalf of MDC. All vendors, contractors, and business partners who store, process, transmit, or have access to cardholder data on behalf of MDC must contractually agree to be compliant with the current version of the PCI DSS during the contract period.

VI. Goals and Applicable Policies and Standards

Payment Card Industry Data Security Standard

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. Below is a high-level overview of the PCI DSS requirements. The complete standard is accessible at: https://www.pcisecuritystandards.org.

A. Goals

Build and Maintain a Secure Network and Systems.

1. Install and maintain Network Security Controls.
2. Apply Secure Configurations to All System Components.

Protect Account Data

3. Protect Stored Account Data.
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.

Maintain a Vulnerability Management Program

5. Protect All Systems and Networks from Malicious Software.
6. Develop and Maintain Secure Systems and Software

Implement Strong Access Control Measures

7. Restrict Access to System Components and Cardholder Data by Business Need to Know.
8. Identify Users and Authenticate Access to System Components.
9. Restrict Physical Access to Cardholder Data.

Regularly Monitor and Test Networks.

10. Log and Monitor All Access to System Components and Cardholder Data.
11. Test Security of Systems and Networks Regularly.

Maintain an Information Security Policy.

12. Support Information Security with Organizational Policies and Programs.

B. Applicable Policies and Procedures

1. 333 - Credit Card Acceptance and Processing Procedures
   https://www.miamidade.gov/managementandbudget/library/procedures/333.pdf
2. 334 – Credit Card Processing Procedures for Working Remotely
   https://intra.miamidade.gov/finance/payment-card-industry.asp
3. PCI Incident Response Plan
   http://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf
4. MDC Enterprise Information Security Policy Manual
   http://intra.miamidade.gov/technology/library/guidelines/security-policy-manual.pdf

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

C. Required Information Security and PCI Training

1. New Employees
    - Security Awareness Essentials
    - Phishing Defense Essentials
    - PCI Essentials for Account Data Handlers and Supervisors Online Training
    - Annual PCI Kick-off Meeting
1. Current Employees (Annually)
    - Phishing Defense Essentials
    - PCI Essentials for Account Data Handlers and Supervisors Online Training
    - Annual PCI Kick-off Meeting

VII. Roles and Responsibilities

A. **Miami-Dade County Entity Directors' processing credit card payments** – are responsible for:

- Assigning a PCI Liaison that is an Accountant 4, equivalent, or higher.
- Managing employees that are responsible for processing, reviewing, reconciling, and approving credit card payments to ensure that they are familiar with and adhere to the PCI DSS requirements of the PCI Security Standards Council.
- Ensuring the employees take the annual mandatory courses as outlined in Section VI.(C).
- Requesting approval from Finance and Information Technology prior to purchase or development of payment application/software to ensure PCI Compliance.
- Including a member of the County PCI Team in any procurement related to payment applications.
- Assigning staff to work and monitor their vendors so they understand and comply with the "Contract Language for Credit Card Payment Systems" for new third-party payment applications prior to executing a contract as described in Procedure #333, section VIII.(A) Contract Language for New Credit Card Payment Systems.

- Ensuring the vendor agrees to be held contractually liable for adherence to the Payment Card Industry compliance for the contract period, including subsequent contract renewals/extensions.
- Ensuring that any change in the credit card environment (payment processor etc.) must be approved by the County's PCI Team prior to implementation.
- Protecting credit card data in compliance with policies referenced in Section VI.(B). Applicable Policies and Procedures found above and the PCI DSS Standards.
- Obtaining certification of PCI compliance for vendor applications, such as, SSF, P2PE validation, or AOC upon expiration date of validation and/or annually. In addition, departments must retain vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and tampering logs. Ensuring that sensitive credit card data is not stored in any form (digitally, hardcopy or voice recording).
    - In an event, a department is unable to obtain a current PCI validation from its third-party vendor annually, and/or by the expiration date, the department must submit to the Finance Administrative and Compliance Services Division a Risk Acceptance Memorandum. *Sample template can be provided.*
- Ensuring the departments ITD support group and/or Business Relationship Manager (BRM) assist in applying patches for applications within 30 days of release for third-party payment systems.
- Work with the assigned systems support group to review all user accounts and related access privileges, including third-party/vendor to ensure appropriate access based on job function responsibilities at least once every six months (PCI Req# 7.2.4).
- Reviewing and taking corrective action on the monthly security scan reports from the Approved Scanning Vendor (ASV) and any other application security scans provided. The department can work with their ITD group/BRM to ensure this occurs.
- Assisting Finance, ITD, and the Qualified Security Assessor (QSA) during the compliance process.
- Reviewing and approving of SAQ, ROC, and AOC for credit card applications annually.

B. **<u>Miami-Dade Entity PCI Liaisons</u> –** are responsible for:

- Ensuring that the responsibilities under the Miami-Dade Entity *Processing Credit Card Payments*, Section VII.(A), as well as those listed in this section are adhered to.
- Adhering to MDC Payment Card Industry Executive Charter and Compliance Policy, in addition to the policies and procedures outlined in Section B above, and the PCI-DSS Standards.
- Reminding department divisions/sections of the requirements regarding prior approvals for purchases of payment applications/software on a quarterly basis.
- Ensuring that POS terminal(s) are recorded on the MID report immediately after receiving the new and/or replacement device.
- Ensuring that all staff involved with the credit card processing functions have had appropriate training which includes a review of all required PCI annual on-line training courses as outlined in Section VI.(C). All required training must be completed annually. Annual certification of training completion must be reviewed and approved by the respective department Director and submitted to the COCC Finance Department.
- Ensuring the County's PCI Team reviews and approves the Scope of Services of any RFP that includes a new/updated system with the capability to process payments.
- Ensuring that any change in the environment (payment processor, server) is communicated and approved by the County's PCI Team.
- Informing employees of any changes and updates with the MDC Payment Card Industry Executive Charter, Credit Card Acceptance and Processing Procedures, and the PCI DSS standards.
- Implementing and annually updating the departmental procedures described in Procedure #333, Credit Card Acceptance and Processing Procedures, including completion of the "Template for Requesting New and Updated Services" and following those guidelines when requesting approval prior to procurement and/or development from the Finance Department to process credit card payments for new services or Merchant Identification Number(s) (MIDs).
- Updating, maintaining, and submitting the Inventory Report semi-annually and/or as changes are made in a central location.

- Assisting Finance and County ITD to confirm the department's PCI-DSS Scope is documented (credit card process, diagram flow, and payment channels) every six months and after a significant change (PCI Req# 12.5.2.1).
- Obtaining certification of PCI compliance for vendor applications, SSF, P2PE validation, or AOC) upon expiration date and/or annually. In addition, departments must retain original vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and tampering logs.
  - In an event, a department is unable to obtain a current PCI validation from its third-party vendor annually, and/or by the expiration date, the department must submit to the Finance, Administrative, and Compliance Services Division a Risk Acceptance Memorandum. *Sample template can be provided.*
- Providing terminal inspection logs and ensuring they are reviewed once a month (even if no evidence of tampering is evident). The inspection of terminals includes all Point of Interaction (POI) devices where payment card data is captured i.e., Pay-on Foot (POF), Point-of-Sale (POS), computers, P2PE terminals, and kiosks etc.
- Assisting Finance, ITD, and the QSA during the compliance process.
- Obtaining department approvals (by the Department Director) on the SAQ and AOC form, as mandated by the PCI DSS.
- In the event of a breach, or suspicion that payment card data has been exposed, lost, stolen, or misused, immediately submit a PCI Incident Report to ITD. The Department's Liaison will work with the County's PCI Team (members from ITD and Finance) and follow the appropriate instructions in accordance with MDC's PCI DSS Incident Response Plan found in MDC's intranet, under the Financial Compliance Section, https://intra.miamidade.gov/finance/payment-card-industry.asp.

C. **Strategic Procurement Department** – is responsible for:

- Ensuring that vendors provide official documentation as listed in Policy 332 MDC Payment Card Industry Executive Charter and Compliance Policy, and the "Contract Language for Credit Card Payment Systems".
- Including the "Contract Language for Credit Card Payment Systems" language in contracts/agreements for credit card payment applications/services. The Payment Card Industry Compliance language

must be included in all RFPs, contracts, and agreements related to credit card payment applications.

- Ensuring that the vendor agrees to be held contractually liable for adherence to the Payment Card Industry compliance for the contract period, including subsequent contract renewals/extensions.
- Ensuring that two PCI Team (Finance and ITD) members are included in each RFP Selection Committee, with at least one (1) voting member and one (1) technical advisor.

D. **Finance Department** – is responsible for:

- Establishing and enforcing policies and procedures for PCI DSS compliance.
- Assisting Miami-Dade Entities with understanding and documenting PCI DSS requirements.
- Providing annual PCI online training and any additional PCI-related training to individual departments/offices as needed.
- Establishing and maintaining relationships with the credit card payment merchant processing provider (currently Elavon).
- Reviewing and approving requests for new credit card services ensuring that processes are in compliance with MDC procedures.
- Working with merchant provider to establish new credit card set up including the new MIDs.
- Working in conjunction with the County ITD on reviewing the documentation for PCI compliance certification.
- Working in conjunction with the County ITD, on approving any POS device or system to be used within MDC.
- Working together with the County ITD to engage the services of a PCI QSA, in consultation with the Clerk of Courts and Comptroller Attorney, County Attorney's Office, and County Strategic Procurement Department.
- Requesting, reviewing, and approving annual updates from each department for credit card procedures, third (3rd) party payment vendor compliance, training, and other documents required for the annual compliance and attestation process.
- Work with Miami-Dade Entities and ITD to review and confirm PCI-DSS scope is documented (credit card process, diagram flow, and payment

channels every six months and after a significant change. PCI Req# 12.5.2.1

- Working in conjunction with ITD, and the QSA during the compliance review process to provide documentation, technical support, respond to inquiries, and conduct on-site visits.
- Obtain completed SAQ and AOC from QSA. Review and distribute to Departments PCI Liaison and Director for their review and approval.
- Approval of final SAQ and AOC by Finance Director.
- Maintaining an updated listing of all departments that process credit card transactions using an approved merchant account.
- Conducting annual/quarterly on-site visits to review processes and assisting departments with PCI Compliance.
- Working together with ITD to conduct annual PCI presentations, training/education.
- Working together with ITD to monitor compliance with this policy.
- Providing an allocation of credit charges to OMB and the departments for budgeting.
- Allocating/billing charges based on actual costs to each department.
- Quarterly Miami-Dade County Entities on-site visits to review credit card procedures and process.
- Quarterly in-person review of roles and responsibility matrix with County ITD staff.

E. **Information Technology Department** – is responsible for:

- Establishing and enforcing policies and procedures for PCI DSS compliance.
- Assisting departments with understanding and implementing PCI DSS technical security requirements.
- Providing annual PCI online training and any additional PCI-related training to individual departments/offices as needed.
- Ensuring that payment applications/software request for procurement through ITD have prior approval from ITD Security and Finance.
- Providing vulnerability assessments, technology reviews, risk assessment, compliance assessment and network segmentation services.

- Work with the departments/elected offices to review all user accounts and related access privileges, including third-party/vendor to ensure appropriate access based on job function responsibilities at least once every six months (PCI Req# 7.2.4).
- Working together with the Finance Department to engage the services of a PCI QSA, in consultation with the County Attorney's Office and Internal Services Department.
- Jointly with the Finance Department, working with the QSA during the compliance review process to provide documentation, respond to inquiries, and conduct on-site visits.
- Jointly with the Finance Department, reviewing documentation for PCI compliance certification.
- Obtain completed SAQ and AOC from QSA. Review documents and obtain approvals for the Service Provider SAQ and AOC.
- Working together with the Finance Department to monitor and audit compliance with this policy.
- Working together with the Finance Department to conduct annual PCI presentations and training/education.
- Working to ensure, upon request, the County provides support to County departments and agencies by:
    - Providing PCI DSS compliance status information (AOC) for services performed on behalf of the Department or agencies.
    - Providing information which PCI DSS requirements are the responsibility of the County and which are the responsibility of the Department or agencies, including any shared responsibilities (Responsibility Matrix, if needed).
- Providing incident response and investigation services for security events impacting the cardholder data environment.
- Monitoring and reviewing computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data.
- Review Targeted Risk Analysis (TRA) Policy annually.
- Annually complete internal and external network penetration testing and application penetration testing.
- Bi-annually complete segmentation penetration testing.

- Complete quarterly internal and external scans. Results are sent to merchant processor.
- Quarterly vulnerability scans and timely fixes to any risks identified.
- Quarterly in-person review of roles and responsibility matrix with County ITD staff.
- Annually update secure build standards and risk assessment.
- Provide online payment application development services:
  - Credit card transaction processing via MDC's Payment Gateway using MDC's credit card processor.

VIII. PCI Compliance Measures of Success

1. Trained staff in the latest PCI DSS standards.

2. Updated and accessible MDC PCI Compliance Policy and Credit Card Processing Procedures.

3. Completed POS Tampering Inspection Logs.

4. Passing scores on ASV's Quarterly Scans.

5. Annual and Semi-Annual completion and follow-up on actionable items on Penetration Test(s).

6. Timely and compliant completion of annual PCI Compliance reporting (SAQs, AOCs, and/or ROC).

IX. Retention and Disposal

Cardholder data shall not be retained/stored electronically or in paper form.

X. Annual PCI DSS Self-Assessment

MDC's PCI Team (Finance and ITD Staff) will contact each department to schedule their annual self-assessment. Each department must have staff available to assist Finance and ITD when the QSA completes their assessment. Each department must complete and have the Department Director approve an annual self-assessment questionnaire to attest compliance with this policy, PCI DSS, and other applicable standards and policies. Departments found not in compliance will need to work to implement appropriate compensating controls or remediation activities.

XI. Response to a Security Breach (Incident Response Plan)

In the event of a breach, or the suspicion that payment card data has been exposed, lost, stolen, or misused, the department must immediately submit a PCI incident report at: https://nsd.miamidade.gov/sr/pciincrep. The County's PCI Team (members from ITD and Finance) will review the incident response report. A member of the County's PCI Team will respond to the departmental PCI Liaison with appropriate instructions in accordance with MDC's PCI DSS Incident Response Plan found at:
https://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf
In addition, refer to the Incident Response Plan for further instructions.

XII. Third Party Vendor Risk Management

Before Miami Dade County executes an agreement with a payment application vendor, or contracts to do business with a vendor for credit card services, the vendor must adhere to the Contract Language for Credit Card Payment Systems; the initiating department must also obtain proof of PCI compliance/certification. The vendor must be held contractually liable for maintaining the PCI certification and all sections of the Contract Language for Credit Card Payment Systems, for the contract period, including subsequent contract renewals/extensions.

Any third-party vendor that processes, transmits, generates, stores, or otherwise accesses credit card data on MDC's behalf must sign MDC's Security Addendum. Departments should work with Strategic Procurement Department to initiate this process.

XIII. Annual Review

This policy will be reviewed on an annual basis in accordance with the PCI Data Security Standards. Departments that process credit card data will submit updated credit card procedures, a SAQ, network diagram, card flow diagram, and a signed AOC annually. Individuals who handle credit card data must complete education specific to the PCI standard annually. In addition, MDC will conduct a risk assessment in connection with PCI compliance that identifies emerging threats and vulnerabilities.

XIV. Credit Card Acceptance and Processing Procedures

Refer to County Policy # 333 regarding applicable procedures for credit card acceptance and processing, as outlined in Section VI, above.

XV. Contract Language for Credit Card Payment Systems

Refer to County procedure # 333, Credit Card Acceptance and Processing Procedures, Section VIII.(A), for requirements applicable to all third-party payment vendor systems. Outlined in Section VI, above.

XVI. PCI Project Calendar

SEPTEMBER

- Procedural on-site visits conducted by Finance Administrative & Compliance Services Division.
- County's PCI Team to finalize updates to MDC PCI Policies and Procedures to include new changes/updates.
- Post Audit work.
- County's PCI Team members (ITD & Finance) meet monthly.
- County's PCI Team to update PCI on-line training course to include new changes.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

OCTOBER

- Post Audit work.
- Procedural on-site visits conducted by Finance Administrative & Compliance Services Division.
- County's PCI Team to complete changes/updated to MDC PCI Policies and Procedures.
- County's PCI Team to complete PCI online training course to include new changes.
- County's PCI Team members (ITD & Finance) meet monthly.
- County's PCI Team to prepare PCI annual presentation.
- ITD conducts Bi-Annual Segmentation Penetration Test, as per PCI requirement 11.4.6. A periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15th of the month and to merchant processor, as per PCI requirements 11.3.1 and 11.3.2. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.4.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.2.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring malware scans are being performed daily as per PCI requirement 5.3.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- The Finance Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to Finance's PCI Team and uploaded into the central location.
- ITD completes a quarterly review ensuring log reviews for all other system components are completed once every seven days, as per PCI requirement 10.4.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD addresses applicable vulnerabilities based on their risk within three months, as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring change and tamper detection mechanisms are deployed to detect unauthorized modifications to payment pages once every seven days, as per PCI requirement 11.6.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- County's PCI Team to finalize PCI On-line training course to include new changes.

NOVEMBER/DECEMBER

- PCI on-line training course available for employees that are responsible for processing, reviewing, reconciling, or approving credit card transactions, process, or systems.
- ITD to update and complete configuration standards.
- County's PCI Team to complete PCI annual presentation.
- County's PCI Team members (ITD & Finance) meet monthly.
- Updates to policies and procedures (Finance & ITD policies).
- Finalize Post Audit recommendation and/or new year PCI requirements.
- Procedural on-site visits conducted by Finance Administrative & Compliance Services Division.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD conducts bi-annual Segmentation Penetration Testing, as per PCI requirement 11.4.6. A periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

JANUARY

- County-wide kick-off meeting for current year credit card procedures, departments PCI compliance, and new year reporting period.
- Departments must submit updated PCI documentation:
  - Credit Card Procedures (SOPs)
  - PCI Compliance from 3rd party payment vendors
  - Updated Technical and Card Flow Diagrams

- MID Listing
- Inventory Report
- POS/POF Device Tampering Log

- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15th of the month and to merchant processor, as per PCI requirements 11.3.1 and 11.3.2. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes an annual malware review, as per PCI requirement 5.2.3.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.4.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.2.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring malware scans are being performed daily as per PCI requirement 5.3.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes an annual review of all access application and system accounts, as per PCI requirement 7.2.5.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a review to ensure passwords/passphrases for application and system accounts are changed every 90 days, as per PCI requirement 8.6.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- Finance Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to Finance's PCI Team and uploaded into the central location.
- ITD completes a quarterly review ensuring log reviews for all other system components are completed once every seven days, as per PCI requirement 10.4.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD addresses applicable vulnerabilities based on their risk within three months, as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring change and tamper detection mechanisms are deployed to detect unauthorized modifications to payment pages once every seven days, as per PCI requirement 11.6.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- Finance Administrative & Compliance Services Division to work with departments to update the following for the new year: credit card policy, MID reports, inventory list, and detailed credit card flows. Annual sign-off sheet with results is uploaded into the central location.
- County's PCI Team members (ITD & Finance) meet bi-weekly.

FEBRUARY

- Miami-Dade Entities' deadline to complete PCI online course.
- Finance Administrative & Compliance Services Division to create a report of Miami-Dade Entity staff that completed PCI Course and provide to PCI Liaisons for review and approval by Department Director.
- Department's deadline to submit approved training reports to Finance and post in PCI central location.
- ITD to conduct Risk Assessment Analysis of cardholder data environment.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- County’s PCI Team members (ITD & Finance) meet bi-weekly.

MARCH

- Finance Administrative & Compliance Services Division to create a Vendor Management listing and file with copies of all third-party vendor applications PCI compliance documents and upload to PCI central location. (Include Compensating Controls, if required).
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- Jointly, Finance and ITD to begin working on annual AOC process with QSA.

APRIL

- Departmental onsite/remote visits with QSA.
- Continue Attestation process.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15th of the month and to merchant processor, as per PCI requirements 11.3.1 and 11.3.2. Periodic sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD completes quarterly monthly review, ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.4.2. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD completes quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI

requirement 11.2.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- ITD completes a quarterly review ensuring malware scans are being performed daily as per PCI requirement 5.3.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- The Finance Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to Finance's PCI Team and uploaded into the central location.
- ITD completes a quarterly review ensuring log reviews for all other system components are completed once every seven days, as per PCI requirement 10.4.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD addresses applicable vulnerabilities based on their risk within three months, as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring change and tamper detection mechanisms are deployed to detect unauthorized modifications to payment pages once every seven days, as per PCI requirement 11.6.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD reviews and updates Targeted Risk Analysis Policy to ensure compliance with PCI requirement 12.3.1.
- County's PCI Team members (ITD & Finance) meet weekly.

MAY

- Continue Attestation and Departmental on-site/remote visits by QSA.
- Finance Administrative & Compliance Services Division to obtain drafts of SAQs from QSA and send to Departments for review and approval by PCI Liaisons.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI

requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- ITD conducts annual internal and external Penetration Testing as per PCI requirements, 11.4.2 and 11.4.3. A periodic sign-off sheet is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD conducts bi-annual Segmentation Penetration Testing, as per PCI requirement 11.4.6. A periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- County's PCI Team members (ITD & Finance) meet weekly.

JUNE

- Finance Administrative & Compliance Services Division section to obtain final SAQ and Attestation documents for review and final signatures by Department Directors.
- Miami-Dade Entity Director/Elected Officer must review and sign SAQ and AOC forms in the first week of June.
- Finance Administrative & Compliance Services Division to obtain final approved forms from Miami-Dade County Entities.
- Obtain approval on final submission forms for merchant processors SAQ/ROCs and Attestation from Finance Director.
- Submission deadline for PCI compliance, submit final forms to Merchant providers through secured email.
- ITD ensures cipher suite and protocols are reviewed and documented on an annual basis, as per PCI requirement 12.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes periodic training for incident response on an annual basis, as per PCI requirement 12.10.4.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- County's PCI Team members (ITD & Finance) meet weekly.

JULY

- Post-compliance review meeting with QSA, senior management, and County's PCI Team.
- Begin work on follow-up items.
- Procedural on-site visits conducted by Finance Administrative & Compliance Services Division.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly internal and external vulnerability scans with summary report. Reports of results are provided to senior management by the 15th of the month and to merchant processor, as per PCI requirements 11.3.1 and 11.3.2. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.2.1. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes quarterly monthly review, ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.4.2. Quarterly sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring malware scans are being performed daily as per PCI requirement 5.3.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- The Finance Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to Finance's PCI Team and uploaded into the central location.
- ITD completes a quarterly review ensuring log reviews for all other system components are completed once every seven days, as per PCI requirement

10.4.2.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

- ITD addresses applicable vulnerabilities based on their risk within three months, as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.
- ITD completes a quarterly review ensuring change and tamper detection mechanisms are deployed to detect unauthorized modifications to payment pages once every seven days, as per PCI requirement 11.6.1. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

AUGUST

- Post Audit work.
- Procedural on-site visits conducted by Finance Administrative & Compliance Services Division.
- County's PCI Team to update MDC PCI Policies and Procedures to include new changes/updates.
- ITD completes monthly security patch management for all system components and software application to credit card environment, as per PCI requirement 6.3.3. Periodic sign-off sheet with results is provided to ITD's PCI Liaison and uploaded into the central location.

XII. Signature Page

Advising Committee (County's PCI Team)

Finance Department

Christopher B. Hill

Christopher Hill, Director, Cash Management Division

Alvaro Carcache, Chief, Administrative & Compliance Services Division

Vivian Delgado, Assistant Director, Finance

Information Technology Department

Ranjana Warier, Senior Security Systems Engineer

Lawrence Embil, Security Systems Manager

Jeremy Clark

Jeremy Clark, Division Director of County Systems

Jonathan Wolfe

Jonathan T. Wolfe, Asst Chief Information Security Officer

Lars Schmekel

Lars Schmekel, Chief Information Security Officer

Strategic Procurement Department

Jessica Tyrrell

Namita Uppal, Director of Strategic Procurement Department

Information Technology – Service Provider

Jorge Mederos, Assistant Director, Enterprise Application Services

Approvals:

Barbara Gomez

Barbara Gomez, Finance Director

Margaret Brisbane

Margaret Brisbane, Director, Information Technology

Dr. Carladenise Edwards, Chief Administrative Officer

Miami-Dade County Departments

Department PCI Liaison	Department Director
Haikel Marrero Haikel Marrero, Animal Services	Annette Jose Annette Jose, Director
Shawn P. Mahoney Shawn Mahoney, Aviation	Ralph Cutie, Director
Karl Ross Karl Ross, Commission on Ethics and Public Trust	Ignacio J VAZQUEZ jR Ignacio J. Vazquez Jr., Executive Director
Nazreen Khan Nazreen Khan, Communications and Customer Experience	Inson Kim Inson Kim, Director
Glorimar Abreu Glorimar Abreu, Community Action & Human Services	Sonia Grice Sonia Grice, Director
Alexander Fernandez Alexander Fernandez, Cultural Affairs	Marialaura Leslie, Director
Jennifer Duque, Emergency Management	Pete Gomez, Director
Darleen Pulido Darleen Pulido, Fire Rescue	Raied "Ray" Jadallah, Fire Chief
Eartha Alexander Eartha Alexander, Public Housing and Community Development	Alex R. Ballina, Director
Ricardo Bran Ricardo Bran, Human Resources	Melanie McLean Melanie McLean, Interim Director
Sara Tippit Sara Tippit, Information Technology	Margaret Brisbane Margaret Brisbane, Director /CIO
Edward R. Muñecas Edward Muñecas, Internal Compliance	Ofelia Tamayo, Director
Kenneth Sapp Kenneth Sapp, Internal Services	Raymond Hall Raymond Hall, Director
Jessica Jarra, Libraries	Ray Baker, Director

JOSE GRANERA

Jose Granera, Parks, Recreation & Open Spaces

Monica Boza

Monica Boza, Regulatory Economic Resources

Andrew Warburton, Seaport

Deborah Silver

Deborah Silver Solid Waste Management

Zunilda Perez, Dept. of Transportation and Public Works

Josephine Barrios, Water and Sewer

Maria L. Nardi, Director

Lourdes M. Gomez

Lourdes M. Gomez, Director

Hydi Webb

Hydi Webb, Director

Aneisha Daniel, PhD, Director

Josiel Ferrer-Diaz, Interim Director

Roy Coley

Roy Coley, Director

Elected Offices

Elected Office PCI Liaison

Jacqueline Williams, Clerk of the Courts and Comptroller

Robert Villar

Robert Villar, Supervisor of Elections

Monica Galo

Monica Galo, Eleventh Judicial Circuit

Nicholas Santos, Sheriff's Office

Ivette Barbeite-Locay

Ivette Barbeite-Locay, Property Appraiser

Yohanka Dominguez

Yohanka Dominguez, Office of the Tax Collector

Director

Barbara Galvez

Barbara Galvez, Director, COCC Administrative Services

Christina White, Supervisor of Elections

Deirdre Dunham

Deirdre Dunham, Trial Court Administrator

S. Daniels

Stephanie V. Daniels, Director

Lazaro Solis

Lazaro Solis, Deputy Property Appraiser

Gerardo Gomez, Interim Director