



**Clerk of the Court and Comptroller
of
Miami Dade County**

332: Payment Card Industry
Executive Charter and
Compliance Policy



**Build and maintain a
secure network**



**Protect cardholder
data**



**Maintain a
vulnerability
management program**



**Implement strong
access control
measures**



**Regularly monitor and
test networks**



**Maintain an
information security
policy**



Table of Contents

Revision to Policy	1
I. Definitions.....	2-4
II. Purpose.....	5
III. Overview	5-
IV. Accountability.....	6
V. Applicability	7
VI. Goals and Applicable Policies and Standards	7
A. Goals.....	7-8
B. Applicable Policies and Standards.....	8
C. Required Information Security and PCI Training	8
VII. Roles and Responsibilities	8-14
A. Miami-Dade County Entity Directors/Constitutional Officers.....	8-10
B. PCI Liaisons	10-11
C. Procurement.....	11-12
D. Comptroller Finance Operations (CFO) Department.....	12-13
E. Communications, Information & Technology (CITD) Department.....	13-14
VIII. PCI Compliance Measures of Success	14
IX. Retention and Disposal.....	15
X. Annual PCI DSS Attestation	15
XI. Response to a Security Breach (Incident Response Plan).....	15
XII. Third-Party Vendor Risk Management.....	15
XIII. Annual Review.....	15
XIV. Credit Card Acceptance and Processing Procedures	16
XV. Contract Language for Credit Card Payment Systems.....	16
XVI. PCI Project Calendar	17-24
XVII. Signature Page	25-28



Revisions to Policy:

This section documents the revisions made to this policy since the last approved version dated October 2025.

Effective Date	Version	Description	Pages
October 2025	332.7.0	Updated cover page	Cover
October 2025	332.7.0	Update name of department and logos	Cover, i – 29
October 2025	332.7.0	Updated Table of Contents	ii
October 2025	332.7.0	Updated various department names	ii – 28
October 2025	332.7.0	Added new terms in Definition Section	1 – 4
October 2025	332.7.0	Updated name of PCI Team	4 – 25
October 2025	332.7.0	General grammatical changes	1-31
October 2025	332.7.0	Added new terms in Definition Section	5
October 2025	332.7.0	Added/updated Roles & Responsibilities Section	8 – 14
October 2025	332.7.0	Updated PCI Liaison Assignment – level of position	8
October 2025	332.7.0	Clarification on PCI Members in Selection Committee	6, 12
October 2025	332.7.0	Added/updated verbiage	5, 10, 16 – 23
October 2025	332.7.0	Added/updated verbiage in PCI Project Calendar	17 – 24
October 2025	332.7.0	Added/updated names in Signature Section	25 – 29



I. Definitions

Acquirer – Also referred to as “merchant bank”, “acquiring bank” or “acquiring financial institution”. Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.

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 (SAQ) or Report on Compliance (ROC).

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” – PCI-SSC-approved vendor who conducts vulnerability scanning and 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 (CHD) - At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. It may include 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.

CFO – to mean the Comptroller Finance Operations Department (CFO) of the Clerk of the Court and Comptroller.

COCC – to mean the Clerk of the Court and Comptroller (COCC) of Miami-Dade County, acting by and through the elected Clerk or his duly authorized officers, agents, or designees.



Constitutional Office – County constitutional officers are independently elected officials in each county and perform specific functions of the county's government.

Customer(s) – to mean Miami-Dade County Departments and Constitutional Offices.

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 Miami-Dade County Entity approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.

Merchant Identification Number – A unique number that identifies the Miami-Dade County Entity approved to accept payment cards.

Miami-Dade County Entity – A county department or constitutional office that accepts credit card as payment.

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.

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.

PCI – Acronym for “Payment Card Industry.”

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

PCI Team – Consists of members of the Clerk’s Comptroller Finance Operations (CFO) Department and Miami-Dade County Communications, Information and Technology (CITD) Department.

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.

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

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.



II. Purpose

The Clerk of the Court and Comptroller (COCC) of Miami-Dade County administers the Payment Card Industry (PCI) Program for compliance with the Payment Card Industry Data Security Standard (PCI DSS). COCC maintains the Payment Card Industry Executive Charter and Compliance Policy, and other supporting credit card compliance procedures. These documents establish the framework for safeguarding cardholder data and maintaining a secure, compliant environment across all participating Miami-Dade County departments and Constitutional Offices.

The Executive Charter's policy is developed in accordance to PCI DSS Req# 12.4.1. The policy assists 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 our customers (Miami-Dade County (MDC) Departments and Constitutional Offices (COs)) processing credit card transactions. PCI Council document library: https://www.pcisecuritystandards.org/document_library/.

III. Overview

There are twenty (20) Miami-Dade County Departments and five (5) Constitutional Offices that we service processing credit card payments at over 200 locations using a variety of payment channels for e-commerce, telephone, and in-person, including but not limited to, Point of Sale (POS) devices, in-house developed applications, third-party payment applications, and interactive voice response (IVR) systems for credit card transactions. Currently there is one main merchant processor and three (3) other merchant processors servicing Departments and Constitutional Offices.

Annually, each Miami-Dade County Entity is required to complete and update its credit card procedures, detailing how transactions are processed in their respective entity. These procedures shall be approved and signed by the Miami-Dade Entity's PCI Liaison and the executive management (Department Director/Constitutional Officer). The updates include credit card procedures, Merchant ID (MID) report, the vendor's PCI compliance certification, technical diagrams, and PCI scope inventory reports. The approved procedures and supporting documentation are submitted to COCC Comptroller Finance Operations (CFO) Department by the respective Miami-Dade Entity's PCI Liaison and posted to the PCI Team secured shared drive. CFO's Administrative & Compliance Services Division will review procedures and MID reports to ensure compliance with policies and PCI DSS requirements. The Communications, Information & Technology Department Security Division (CITD) reviews the PCI certification, technical diagrams, and PCI scope inventory reports for compliance with PCI, technical, and security



policies/procedures. Both CFO and CITD PCI Team members work in conjunction to secure compliance for the Miami Dade Entity's.

Miami-Dade Entities submitting new requests to process credit card transactions, or requests regarding changes in current credit card processes, must resubmit their new proposed procedures for review and approval, prior to procurement and implementation.

A review of internal controls and compliance with PCI-DSS is completed and reviewed for approval by the PCI Team. Two members of the PCI Team must be part of the Request for Proposal (RFP) for any solicitations that involve systems with the capability to process payments, and at least one shall be a voting member and the other shall be a technical advisor of the Selection Committee.

CITD conducts monthly internal scans based on inventory reports, as provided by each Miami-Dade Entity 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) and Senior Management. Internal and external penetration tests are performed annually and after any significant infrastructure or application upgrade or change. Bi-annual PCI segmentation tests, application penetration tests, and targeted risk assessments are completed to identify any threats and/or vulnerabilities requiring remediation. Quarterly field visits are conducted by the CFO's Administrative & Compliance Services Division to monitor and assist each Miami-Dade County Entity with PCI compliance.

IV. Accountability

Miami-Dade County Entities processing credit card transactions are required to adhere and comply with all applicable policies and procedures. Miami-Dade County Entity Directors/Constitutional Officers have full oversight over their respective Miami-Dade Entity and provide appropriate Miami-Dade Entity approvals including those of the Self-Assessment Questionnaire (SAQ), Report on Compliance (ROC), and the Attestation of Compliance (AOC).

CFO reviews and monitors PCI compliance and applicable policies and procedures. County CITD reviews and monitors Departmental PCI compliance with technology related guidelines/regulations. Each Department Director approves their portion of the SAQ/ROC and AOC. The CFO Department Director approves the countywide SAQ/ROC and AOC that is submitted to the merchant processors. The Constitutional Officer approves SAQ/ROC and AOC for their respective office.

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 Miami-Dade County Entity who contracts with a third-party vendor to handle and/or process cardholder data on their behalf. All vendors, contractors, and business partners who store, process, transmit, or have access to cardholder data on behalf of Miami-Dade County Entity must contractually agree to be compliant with the current version of the PCI DSS during the contract period.

VI. Standard and Requirements and Applicable Policies

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. PCI DSS Standard and Requirements

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
2. 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/Constitutional Officers – are responsible for:

1. Assigning a PCI Liaison who can understand the related issues and can effectively discuss with executive management, with qualifications equivalent to a mid-to-upper-level accountant.
2. 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.



3. Ensuring the employees take the annual mandatory courses as outlined in Section VI(C).
4. Requesting approval from CFO and Communications, Information & Technology (CITD) prior to purchase or development of payment application/software to ensure PCI Compliance.
5. Including a member of the PCI Team in any procurement related to payment applications.
6. 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.
7. 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.
8. Ensuring that any change in the credit card environment (payment processor etc.) must be approved by the PCI Team prior to implementation.
9. Protecting credit card data in compliance with policies referenced in Section VI(B). Applicable Policies and Procedures found above and the PCI DSS Standards.
10. 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, Miami-Dade Entities 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).
 - a. In an event, a Miami-Dade Entity is unable to obtain a current PCI validation from its third-party vendor annually, and/or by the expiration date, they must submit to the CFO's Administrative and Compliance Services Division a Risk Acceptance Memorandum. *Sample template can be provided.*
11. Ensuring the Miami-Dade Entities CITD support group and/or Business Relationship Manager (BRM) assist in applying patches for applications within 30 days of release for third-party payment systems.
12. 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).
13. 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 Miami-Dade Entity can work with their CITD group/BRM to ensure this occurs.



14. Assisting CFO, CITD, and the Qualified Security Assessor (QSA) during the compliance process.
15. Reviewing and approving of SAQ, ROC, and AOC for credit card applications annually.

B. PCI Liaisons – are responsible for:

1. Ensuring that the responsibilities under the Miami-Dade County Entity Roles and Responsibilities as well as those listed in this section are adhered to.
2. Adhering to the Clerk's Payment Card Industry Executive Charter and Compliance Policy, in addition to the policies and procedures outlined in Section VI (B) of this document, and the PCI-DSS Standards.
3. Reminding Miami-Dade Entity divisions/sections of the requirements regarding prior approvals for purchases of payment applications/software on a quarterly basis.
4. Ensuring that POS terminal(s) are recorded on the MID report immediately after receiving the new and/or replacement device.
5. Ensuring that all staff involved with the credit card processing functions have had appropriate training which includes all required PCI annual on-line training courses as outlined in *Required Information Security and PCI Training, Section VI(C)*. All required training must be completed annually. Annual certification of training completion must be reviewed and approved by the respective Miami-Dade County Entity Executive Management and submitted to the CFO.
6. Ensuring the PCI Team reviews and approves the Scope of Services of any RFP that includes a new/updated system with the capability to process payments.
7. Ensuring that any change in the environment (payment processor, server) is communicated and approved by the PCI Team.
8. Informing employees of any changes and updates with the Clerk's Payment Card Industry Executive Charter, Credit Card Acceptance and Processing Procedures, and the PCI DSS standards.
9. Implementing and annually updating their credit card 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 CFO to process credit card payments for new services or Merchant Identification Number(s) (MIDs).
10. Updating, maintaining, and submitting the Inventory Report semi-annually and/or as changes are made in a central location.



11. Assisting CFO and CITD to confirm the Miami-Dade Entity'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*)
12. Obtaining certification of PCI compliance for vendor applications, SSF, P2PE validation, or AOC) upon expiration date and/or annually. In addition, Miami-Dade Entities must retain original vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and tampering logs.
 - a. In an event, a Miami-Dade Entity is unable to obtain a current PCI validation from its third-party vendor annually, and/or by the expiration date, they must submit to the CFO's Administrative, and Compliance Services Division a Risk Acceptance Memorandum. *Sample template can be provided.*
13. Providing device inspection logs and ensuring they are reviewed at least once a month (even if no evidence of tampering is evident). The inspection of devices includes all Point of Interaction (POI) devices where payment card data is captured i.e., Pay-on Foot (POF), TVMs, Point-of-Sale (POS), computers, P2PE terminals, and kiosks etc.
14. Assisting CFO, CITD, and the QSA during the compliance process.
15. Obtaining approvals by the Director/Constitutional Officer on the SAQ and AOC form, as mandated by the PCI DSS.
16. 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 CITD. The Miami-Dade Entity's Liaison will work with the PCI Team and follow the appropriate instructions in accordance with the Clerk's PCI DSS Incident Response Plan found in CFO's intranet website, under the Financial Compliance Section, <https://intra.miamidade.gov/finance/payment-card-industry.asp>.

C. Procurement – is responsible for:

1. Ensuring the below procedures are followed for contracts involving credit card payment processing.
2. Including in the Contracts documentation as listed in the Clerk's Payment Card Industry Executive Charter and Compliance Policy 332, and the "Contract Language for Credit Card Payment Systems".
3. 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, even if the credit card module will not be implemented.
4. Verifying that the PCI Team has reviewed and approved the Scope of Work.



5. Including Contract language that holds the vendor contractually liable for adherence to the Payment Card Industry compliance for the contract period, including subsequent contract renewals/extensions.
6. Ensuring that two PCI Team (CFO and CITD) members are included in each RFP Selection Committee, with at least one (1) voting member and one (1) technical advisor.

D. Comptroller Finance Operations (CFO) Department – is responsible for:

1. Establishing and enforcing policies and procedures for PCI DSS compliance.
2. Assisting our customers with understanding and documenting PCI DSS standards and requirements.
3. Providing annual PCI online training and any additional PCI-related training to Miami-Dade Entities as needed.
4. Establishing and maintaining relationships with the credit card payment merchant processing provider.
5. Reviewing and approving requests for new credit card services ensuring that processes are complying with the Clerk's PCI Charter and procedures.
6. Working with merchant provider to establish new credit card set up including the new MIDs.
7. Working in conjunction with CITD on reviewing the documentation for PCI compliance certification.
8. Working in conjunction with CITD, on approving any POS device or system to be used by Miami-Dade Entities.
9. Working together with the CITD to engage the services of a PCI QSA, in consultation with the Clerk of Court and Comptroller Attorney, County Attorney's Office, and Procurement Department.
10. Requesting, reviewing, and approving annual updates from each Miami-Dade Entity for credit card procedures, third (3rd) party payment vendor compliance, training, and other documents required for the annual compliance and attestation process.
11. Work with Miami-Dade Entities and CITD 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)*)
12. Working in conjunction with CITD, and the QSA during the compliance review process to provide documentation, technical support, respond to inquiries, and conduct on-site visits.
13. Obtain completed SAQ and AOC from QSA. Review and distribute to Miami-Dade Entities PCI Liaison and Director/Constitutional Officer for their review and approval.



14. Approval of final SAQ and AOC by CFO Director.
15. Maintaining an updated listing of all Miami-Dade Entities that process credit card transactions using an approved merchant account.
16. Conducting annual/quarterly on-site visits to review procedures, processes and assisting Miami-Dade Entities with PCI Compliance.
17. Working together with CITD to conduct annual PCI presentations, training/education.
18. Working together with CITD to monitor compliance with this policy.
19. Providing an allocation of credit charges to County's OMB and the Miami-Dade Entities for budgeting.
20. Allocating/billing charges based on actual costs to each Miami-Dade Entity.
21. Quarterly review of Miami-Dade Entities device inspection logs to ensure periodic monthly inspections and documentation is properly maintained.
22. Quarterly in-person review of roles and responsibility matrix with CITD staff.
23. Review Targeted Risk Analysis (TRA) Policy annually. (*PCI Req# 12.3.1*)

E. Communications, Information & Technology (CITD) Department – is responsible for:

1. Establishing and enforcing policies and procedures for PCI DSS compliance.
2. Assisting Miami-Dade Entities with understanding and implementing PCI DSS technical security requirements.
3. Providing annual PCI online training and any additional PCI-related training to Miami-Dade Entities as needed.
4. Ensuring that payment applications/software request for procurement have prior approval from CITD Security and CFO.
5. Providing vulnerability assessments, technology reviews, risk assessment, compliance assessment and network segmentation services.
6. Work with the Miami-Dade Entities 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*).
7. Review all system and application accounts and related access privileges annually. (*PCI Req# 7.2.5 and 7.2.5.1*)
8. Working together with CFO to engage the services of a PCI QSA.
9. Jointly with CFO, working with the QSA during the compliance review process to provide documentation, respond to inquiries, and conduct on-site visits.
10. Jointly with CFO, reviewing documentation for PCI compliance certification.



11. Obtain completed SAQ and AOC from QSA. Review documents and obtain approvals for the Service Provider SAQ and AOC.
12. Working together with CFO to monitor and audit compliance with this policy.
13. Working together with the CFO to conduct annual PCI presentations and training/education.
14. Working to support customers by:
 - a. Providing PCI DSS compliance status information (AOC) for services performed on behalf of the Miami-Dade County Entities.
 - b. Providing information which PCI DSS requirements are the responsibility of CITD and, by extension, are the responsibility of the Miami-Dade Entity, including any shared responsibilities (Responsibility Matrix, if needed).
15. Providing incident response and investigation services for security events impacting the cardholder data environment.
16. Monitoring and reviewing computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data.
17. Review Targeted Risk Analysis (TRA) Policy annually. (*PCI Req# 12.3.1*)
18. Annually complete internal and external network penetration testing and application penetration testing.
19. Bi-annually complete segmentation penetration testing.
20. Complete quarterly internal and external scans. Results are sent to merchant processor.
21. Quarterly vulnerability scans and timely fixes to any risks identified (High Risk or Critical).
22. Quarterly in-person review of roles and responsibility matrix with CITD staff.
23. Annually update secure build standards and risk assessment.
24. Provide online payment application development services:
 - a. Credit card transaction processing via County's Payment Gateway using approved merchant processor.

VIII. PCI Compliance Measures of Success

1. Trained staff in the latest PCI DSS standards.
2. Updated and accessible PCI Compliance Policy and Credit Card Processing Procedures.
3. Completed Device 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 or ROCs, and AOCs).



IX. Retention and Disposal

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

X. Annual PCI DSS Attestation

The PCI Team will contact each Miami-Dade Entity to schedule their annual compliance audit. Each Miami-Dade Entity will assign staff to assist during the audit. Each Miami-Dade Entity must review and have the Department Director/Constitutional Officer approve an annual SAQ/ROC and AOC to attest compliance with this policy, PCI DSS, and other applicable standards and policies as noted on the forms. Under certain circumstances, Miami-Dade Entities may be asked 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 Miami-Dade Entity must immediately submit a PCI incident report at: <https://nsd.miamidade.gov/sr/pciincprep>. The PCI Team will review the incident response report. A member of the PCI Team will respond to the Miami-Dade Entity PCI Liaison with appropriate instructions in accordance with the Clerk'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 a Miami-Dade Entity executes a contractual agreement with a payment application vendor to do business with for credit card services, the vendor must adhere to the Contract Language for Credit Card Payment Systems; the initiating Miami-Dade Entity 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 the Miami-Dade Entity's behalf must sign MDC's Security Addendum. Miami-Dade Entities should work with the Procurement Department to initiate this process and provide the PCI Team with a Scope of Work for review.

XIII. Annual Review

This policy will be reviewed on an annual basis in accordance with the PCI Data Security Standards. Miami-Dade Entities 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 training specific to the PCI standard annually. In addition, an annual Risk Assessment will be conducted in connection with PCI compliance that identifies emerging threats and vulnerabilities.



XIV. Credit Card Acceptance and Processing Procedures

Refer to the COCC's Procedure #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 the COCC's 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 CFO Administrative & Compliance Services Division.

PCI Team to finalize updates to COCC PCI Executive Charter and Procedures to include new changes/updates.

Post Audit work.

PCI Team meets monthly.

PCI Team to update PCI online training course to include new changes.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

OCTOBER

Post Audit work.

Procedural on-site visits conducted by CFO Administrative & Compliance Services Division.

PCI Team to complete changes/updated to COCC PCI Executive Charter and Procedures.

PCI Team to complete PCI online training course to include new changes.

PCI Team meets monthly.

PCI Team to prepare PCI annual presentation.

CITD reviews configurations of Network Security Controls (NSCs) at least every six (6) months to confirm they are relevant and effective, as per PCI requirement 1.2.7. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD conducts Bi-Annual Segmentation Penetration Test, as per PCI requirement 11.4.6. A periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly internal 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 requirement 11.3.1. CITD addresses and rescan High-Risk or Critical vulnerabilities to be resolved. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.



CITD completes quarterly 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 requirement 11.3.2. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

The CFO Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per MDC TRA Policy for PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD addresses applicable vulnerabilities based on their risk. Medium: within three months; Low: within six months; Informational: Monitor regularly as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

PCI Team to finalize PCI Online training course to include new changes.

NOVEMBER/DECEMBER

PCI online training course available for employees that are responsible for processing, reviewing, reconciling, or approving credit card transactions, process, or systems.

CITD to update and complete configuration standards.

PCI Team to complete PCI annual presentation.

PCI Team meets monthly.

PCI Team updates to policies and procedures.

Finalize Post Audit recommendation and/or new year PCI requirements.

Procedural on-site visits conducted by CFO Administrative & Compliance Services Division.

CITD 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 PCI Team and uploaded into the CITD central shared folder.



CITD conducts bi-annual Segmentation Penetration Testing, as per PCI requirement 11.4.6. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

JANUARY

County-wide kick-off meeting for current year credit card procedures, Miami-Dade Entities PCI compliance, and new year reporting period.

Miami-Dade Entities must submit updated PCI documentation:

- Credit Card Procedures (SOPs)
- PCI Compliance from 3rd party payment vendors
- Shared Responsibility Matrix (Roles and Responsibilities)
- Updated Technical and Card Flow Diagrams
- MID Listing (including POS device inventory)
- PCI Scope Inventory Report
- POS/POF Device Tampering Log

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly internal 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 requirement 11.3.1. CITD addresses and rescans High-Risk or Critical vulnerabilities to be resolved. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly 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 requirement 11.3.2. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD completes an annual malware review, as per PCI requirement 5.2.3.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly review ensuring personnel are following security policies and operational procedures, as per PCI requirement 12.4.2. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.



CITD 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 PCI Team and uploaded into the CITD central shared folder.

CFO Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per MDC TRA Policy for PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to CFO's PCI Team and uploaded into the central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD addresses applicable vulnerabilities based on their risk. Medium: within three months; Low: within six months; Informational: Monitor regularly, as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CFO Administrative & Compliance Services Division to work with Miami-Dade Entities 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 shared folder.

PCI Team meets bi-weekly.

FEBRUARY

Miami-Dade Entities' deadline to complete PCI online course.

CFO 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 Miami-Dade Entities Directors/Constitutional Officer.

Miami-Dade Entities' deadline to submit approved training reports to CFO and upload in PCI central location.

CITD to conduct Risk Assessment Analysis of cardholder data environment.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

PCI Team meets bi-weekly.

MARCH

CFO's 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 shared folder. (Include Compensating Controls, if required).



CITD 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 PCI Team and uploaded into the CITD central shared folder.

Jointly, CFO and CITD to begin working on annual AOC process with QSA.

APRIL

Departmental onsite/remote visits with QSA.

Continue Attestation process.

CITD reviews configurations of Network Security Controls (NSCs) at least every six (6) months to confirm they are relevant and effective, as per PCI requirement 1.2.7. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly internal 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 requirement 11.3.1. CITD addresses and rescan High-Risk or Critical vulnerabilities to be resolved. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly 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 requirement 11.3.2. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

The CFO Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per MDC TRA Policy for PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to CFO's PCI Team and uploaded into the central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.



CITD addresses applicable vulnerabilities based on their risk. Medium: within three months; Low: within six months; Informational: Monitor regularly as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD reviews and updates Targeted Risk Analysis Policy to ensure compliance with PCI requirement 12.3.1.

PCI Team meets weekly.

MAY

Continue Attestation and Departmental on-site/remote visits by QSA.

CFO's Administrative & Compliance Services Division to obtain drafts of SAQs from QSA and send to Departments for review and approval by PCI Liaisons.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD conducts annual internal and external Penetration Testing as per PCI requirements, 11.4.2 and 11.4.3. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD conducts bi-annual Segmentation Penetration Testing, as per PCI requirement 11.4.6. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

PCI Team meets weekly.

JUNE

CFO's Administrative & Compliance Services Division section to obtain final SAQ and Attestation documents for review and final signatures by Department Directors.

Miami-Dade Entity Director/Constitutional Officer must review and sign SAQ and AOC forms in the first week of June.

CFO's 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.



CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

PCI Team meets weekly.

JULY

Post-compliance review meeting with QSA, senior management, and PCI Team.

Begin work on follow-up items.

Procedural on-site visits conducted by CFO's Administrative & Compliance Services Division.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly internal 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 requirement 11.3.1. CITD addresses and rescan High-Risk or Critical vulnerabilities to be resolved. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD completes quarterly 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 requirement 11.3.2. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.



The CFO Administrative & Compliance Services Division completes a quarterly review to ensure device inspections are completed once every month, as per MDC TRA Policy for PCI requirement 9.5.1.2.1. Periodic sign-off sheet with results is provided to CFO's PCI Team and uploaded into the central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

CITD addresses applicable vulnerabilities based on their risk. Medium: within three months; Low: within six months; Informational: Monitor regularly as per PCI requirement 11.3.1.1. Periodic sign-off sheet with results is provided to PCI Team and uploaded into the CITD central shared folder.

CITD 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 PCI Team and uploaded into the CITD central shared folder.

AUGUST

Post Audit work.

Procedural on-site visits conducted by CFO's Administrative & Compliance Services Division.

PCI Team to update the COCC's PCI Charter and Procedures to include new changes/updates.

CITD 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 PCI Team and uploaded into the CITD central shared folder.



XII. Signature Page

Note: Compliance policy changes from last year to this year are noted in **Revisions to Policy** on page 1 of this document.

PCI Team

**Clerk of the Court and Comptroller
Comptroller Finance Operations Department**

Katherine Sosa

Katherine Sosa, PCI Compliance Administrator

Christina Torres

Christina Torres, PCI Compliance Administrator

Alvaro Carcache

Alvaro Carcache, Chief, Administrative &
Compliance Services Division

**Miami-Dade County
Communications, Information & Technology
Department**

Jeremy Clark

Jeremy Clark, Division Director of County Systems

Lawrence Embil

Lawrence Embil, Security Systems Manager

Procurement

Namita Uppal

Namita Uppal, Director of Strategic Procurement
Department

Newton Blanc

Newton Blanc, Procurement Manager
Office of the Tax Collector

Isaura Berrios

Isaura V Berrios, Procurement Manager
Sheriff's Office

Basia Pruna

Basia Pruna, Director, Clerk of the Board &
Procurement

Clerk of the Court and Comptroller
JC Romano

Juan C. Romano, Procurement Manager
Office of the Property Appraiser



Approvals

Vivian Delgado

Vivian Delgado, Deputy Director
Comptroller Finance Operations Department

Barbara Gomez

Barbara Gomez, Director
Comptroller Finance Operations Department

Barbara Galvez

Barbara Galvez, COCC Chief Administrative Officer
Clerk of the Court and Comptroller of Miami-Dade
County

Jorge Mederos

Jorge Mederos, Assistant Director
Communications, Information & Technology
Department

Carladenise Edwards

Dr. Carladenise Edwards, Chief Administrative Officer
Miami-Dade County

Jimmy Morales
Jimmy Morales, Chief Operating Officer
Miami-Dade County



Miami-Dade County Constitutional Offices

Constitutional Office PCI Liaison


Jacqueline Williams, Clerk of the Court and
Comptroller

Federico Arana, Supervisor of Elections

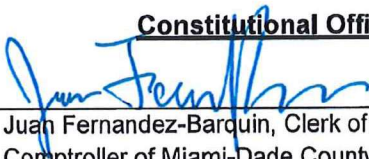
Yohanka Dominguez, Office of the Tax Collector

Nicholas Santos, Sheriff's Office

Casey Simpkins, Office of the Property Appraiser

Monica Galo, Eleventh Judicial Circuit

Constitutional Officer


Juan Fernandez-Barquin, Clerk of the Court and
Comptroller of Miami-Dade County

Alina Garcia, Supervisor of Elections

Daniel Fernandez, Tax Collector

Rosie Cordero-Stutz, Sheriff

Tomas Regalado, Property Appraiser

Deirdre Dunham, Trial Court Administrator



Miami-Dade County Constitutional Offices

Constitutional Office PCI Liaison

Jacqueline Williams, Clerk of the Court and
Comptroller

Federico Arana, Supervisor of Elections

Yohanka Dominguez, Office of the Tax Collector

Nicholas Santos, Sheriff's Office

Casey Simpkins, Office of the Property Appraiser

Monica Galo, Eleventh Judicial Circuit

Constitutional Officer

Juan Fernandez-Barquin, Clerk of the Court and
Comptroller of Miami-Dade County

Alina Garcia, Supervisor of Elections

Daniel Fernandez, Tax Collector

Rosie Cordero-Stutz, Sheriff

Tomas Regalado, Property Appraiser

Deirdre Dunham, Trial Court Administrator



Miami-Dade County Constitutional Offices

Constitutional Office PCI Liaison

Jacqueline Williams, Clerk of the Court and
Comptroller

Federico Arana, Supervisor of Elections

Yohanka Dominguez, Office of the Tax Collector


Nicholas Santos, Sheriff's Office

Casey Simpkins, Office of the Property Appraiser

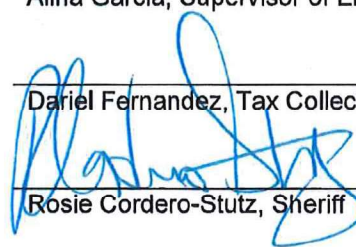
Monica Galo, Eleventh Judicial Circuit

Constitutional Officer

Juan Fernandez-Barquin, Clerk of the Court and
Comptroller of Miami-Dade County

Alina Garcia, Supervisor of Elections

Daniel Fernandez, Tax Collector


Rosie Cordero-Stutz, Sheriff

Tomas Regalado, Property Appraiser

Deirdre Dunham, Trial Court Administrator



Miami-Dade County Constitutional Offices

Constitutional Office PCI Liaison

Jacqueline Williams, Clerk of the Court and
Comptroller

Federico Arana, Supervisor of Elections

Yohanka Dominguez, Office of the Tax Collector

Nicholas Santos, Sheriff's Office

Casey Simpkins

Casey Simpkins, Office of the Property Appraiser

Monica Galo, Eleventh Judicial Circuit

Constitutional Officer

Juan Fernandez-Barquin, Clerk of the Court and
Comptroller of Miami-Dade County

Alina Garcia, Supervisor of Elections

Dariel Fernandez, Tax Collector

Rosie Cordero-Stutz, Sheriff

Tomas Regalado

Tomas Regalado, Property Appraiser

Deirdre Dunham, Trial Court Administrator



Miami-Dade County Constitutional Offices

Constitutional Office PCI Liaison

Jacqueline Williams, Clerk of the Court and
Comptroller

Federico Arana, Supervisor of Elections

Yohanka Dominguez, Office of the Tax Collector

Nicholas Santos, Sheriff's Office

Casey Simpkins, Office of the Property Appraiser

Monica Galo, Eleventh Judicial Circuit

Constitutional Officer

Juan Fernandez-Barquin, Clerk of the Court and
Comptroller of Miami-Dade County

Alina Garcia, Supervisor of Elections

Dariel Fernandez, Tax Collector

Rosie Cordero-Stutz, Sheriff

Tomas Regalado, Property Appraiser

Deirdre Dunham, Trial Court Administrator



Miami-Dade County Departments

Department PCI Liaison

Haikel Marrero

Haikel Marrero, Animal Services
Shawn P. Mahoney, CPA

Shawn Mahoney, Aviation
Karl Ross

Karl Ross, Commission on Ethics and Public Trust
glorimar abreu
Glorimar Abreu, Community Services Department

Alexander Fernandez
Alexander Fernandez, Cultural Affairs
John

Jennifer Duque, Emergency Management
Eartha Alexander
Eartha Alexander, Housing and Community
Development
Darleen Pulido

Darleen Pulido, Fire Rescue
Melissa Belmonte

Melissa Belmonte, Communication, Information &
Technology
Edward R. Muñecas

Edward Muñecas, Internal Compliance
Kenneth Sapp

Kenneth Sapp, People & Internal Operations

Department Director

Annette Jose

Annette Jose, Director
Ralph Cutie

Ralph Cutie, Director
Ignacio J. Vázquez, Jr.

Ignacio J. Vazquez Jr., Executive Director
Cathy Burgos
Cathy Burgos, Director

Ashlee Thomas
Ashlee Thomas, Interim Director
Pete Gomez

Pete Gomez, Director
Nathan Kogon
Nathan Kogon, Director

Raied "Ray" Jadallah
Raied "Ray" Jadallah, Fire Chief

Jorge Olazabal
Jorge Olazabal, Director / Chief Information Officer

Ofelia Tamayo
Ofelia Tamayo, Director

Mariaelena Salazar
Mariaelena Salazar, Interim Director



Miami-Dade County Departments

Department PCI Liaison

Annette Perez, Libraries
Jose Granera

Jose Granera, Parks, Recreation & Open Spaces

Monica Boza, Regulatory Economic Resources

Andrew Warburton, Seaport

Christene Seymour, Solid Waste Management

Rodney Marsh, Dept. of Transportation and Public Works

Josephine Barrios, Water and Sewer

Tiffany Machado, Office of Intergovernmental Affairs

Department Director

Ray Baker, Director

Christina White, Director
Lourdes Gomez

Lourdes M. Gomez, Director
Hydi Webb

Hydi Webb, Director

Aneisha Daniel, PhD, Director

Stacy Miller, Director/CEO

Jay Fink, Director

Alina Gonzalez, Director