# Table of Contents

I. Purpose .........................................................................................................................2

II. Overview.......................................................................................................................2

III. Definitions...................................................................................................................3

IV. Accountability.............................................................................................................5

V. Applicability................................................................................................................5

VI. Goals and Applicable Policies and Standards.............................................................6

VII. Roles and Responsibilities........................................................................................7

   A. Departments.............................................................................................................7

   B. Department’s PCI Liaison.......................................................................................8

   C. Internal Services....................................................................................................9

   D. Finance..................................................................................................................9

   E. Information Technology.........................................................................................10

VIII. PCI Compliance Measures of Success....................................................................11

IX. Retention and Disposal..............................................................................................12

X. Annual PCI-DSS Assessment.....................................................................................12

XI. Response to a Security Breach................................................................................12

XII. Third Party Vendor Risk Management...................................................................12

XIII. Annual Review.......................................................................................................13

XIV. Credit Card Acceptance and Processing Procedures............................................13

XV. Contract Language for Credit Card Payment System............................................13

XVI. PCI Project Calendar...............................................................................................14

XVII. Signature Page.......................................................................................................20
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/agencies processing credit card transactions as required by PCI DSS #12.4.1.

II. Overview

MDC processes more than five million transactions annually accounting for over $460 million dollars in credit card payments to MDC. There are twenty-two (22) departments/agencies in MDC that process credit card payments at over 180 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.

Annually, each department 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 PCI SharePoint (shared file access point). The Cash Management and the Compliance Section of the Finance Director’s office will review procedures to ensure compliance with County’s Policy and PCI requirements. The Information Technology Department (ITD) reviews PCI certification, technical diagrams and inventory reports to review compliance with PCI, technical, and security policies/procedures.

New department requests to process credit card transactions or changes in processes requires resubmittal of procedures to be approved. 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 Finance Department.

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 are submitted to County processor(s). Annual internal and external penetration testing and risk assessment are completed to identify any threats and/or vulnerabilities requiring remediation. Bi-annual field visits are conducted by the Finance Compliance section to monitor for and assist departments with PCI compliance.

III. Definitions

**Account Number** – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “PAN” or “Primary Account Number”.

**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.

**ASV** – “Approved Scanning Vendor” - vendor which 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”.

**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.

**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 or dip) 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.”

**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 Payment Application Data Security Standard (PA DSS). 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/](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.


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.

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

MDC departments 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 as such provide appropriate approvals including those of the SAQ and AOC. The Finance department reviews and monitors departmental PCI compliance and applicable policies and procedures. ITD reviews and monitors departmental PCI compliance and compliance with technology related guidelines/regulations. The Deputy Mayor/Finance Director approves the countywide AOC.

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 employee 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 the [PCI Security Council website](https://www.pcisecuritycouncil.org).

A. Goals

**Build and maintain secure network and systems.**
1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

**Maintain a Vulnerability Management Program**
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

**Implement Strong Access Control Measures**
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

**Regularly monitor and test networks.**
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

**Maintain an Information Security Policy.**
12. Maintain a policy that addresses information security for all personnel.
B. Applicable Policies and Procedures

Miami Dade County
ITD Information Security Policy Manual
Miami Dade County Identity Theft Prevention Program (Red Flags) - Resolution R-580-10

VII. Roles and Responsibilities

A. Departments processing credit card payments – are responsible for:

- Assigning a PCI Liaison;
- Management and employees responsible for processing, reviewing, reconciling, and approving credit card payments must be familiar with and adhere to the PCI DSS requirements of the PCI Security Standards Council; management must also ensure employees take the annual mandatory PCI Training Course;
- Ensure vendors adhere to “Contract Language for Credit Card Payment Systems” for new third-party payment applications prior to executing a contract;
- Implementing the business procedures described in Procedure #333, Credit Card Acceptance and Processing Procedures, including completion of the “Template for New and Updated Credit Card Procedures” and following those guidelines when requesting approval from the Finance Department to process credit card payments for new services (Merchant Identification Number (MID’s) requests);
- Protecting credit card data in compliance with the MDC Payment Card Industry Executive Charter and Compliance Policy and the PCI DSS Standards;
- Reviewing and updating departmental procedures annually in accordance with established guidelines;
- On an annual basis, obtain certification of PCI compliance for vendor applications, such as, PA DSS, P2PE validation, or AOC. In addition, departments must retain vendor PCI related documentation, including but not limited to credit card diagrams/flow, policies, procedures, and logs;
- Ensuring that sensitive credit card data is not stored in any form (digitally, hardcopy or voice recording);
• For third-party payment systems, apply patches for applications within 30 days of release;
• Reviewing and taking corrective action on the monthly security scan reports from the ASV and any other application security scans provided;
• Regularly checking Point of Sale (POS) devices for tampering (skimmers) and documenting/logging findings (even if no evidence of tampering is evident);
• Assisting Finance, ITD, and the QSA during the compliance process.;
• Annual Review and approval of SAQ, ROC, and AOC for credit card applications.

B. Department PCI Liaison’s – are responsible for:
• Adhering to MDC Payment Card Industry Executive Charter and Compliance Policy and the PCI-DSS Standards;
• Ensuring that all staff involved with the credit card processing functions has had appropriate training which includes a review of the PCI annual on-line training course, ITD Information Security awareness course, and the Phishing course; such trainings must be completed annually. Annual certification of training completion must be submitted to the Finance Department and approved by the respective department Director;
• Informing employees of any changes and updates with the MDC Payment Card Industry Executive Charter and Compliance Policy and the PCI DSS standards;
• Implementing the business procedures described in Procedure #333, Credit Card Acceptance and Processing Procedures, including completion of the “Template for New and Updated Credit Card Procedures” and following those guidelines when requesting approval from the Finance Department to process credit card payments for new services or Merchant Identification Number(s) (MID’s);
• Updating departmental procedures annually in accordance with established guidelines;
• Updating, maintaining and uploading PCI device inventory semi-annually and as changes are made in a central location;
• On an annual basis, obtain certification of PCI compliance for vendor applications, such as, PA DSS, P2PE validation) or AOC. In addition, departments must retain vendor PCI related documentation, including
but not limited to credit card diagrams/flow, policies, procedures, and logs;

- Providing terminal inspection logs and ensuring that these are reviewed at least quarterly (even if no evidence of tampering is evident);
- 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 the 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 PCI Core Team (members from ITD and Finance) and follow the appropriate instructions in accordance with MDC’s PCI DSS Incident Response Plan found in the PCI SharePoint.

C. **Internal Services 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 RFP’s, 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.

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

- Establishing and enforcing policies and procedures for PCI DSS compliance;
- Assisting departments with understanding and documenting PCI DSS requirements;
- Establishing and maintaining relationships with the credit card payment merchant processing provider (currently Elavon);
- Reviewing and approving request 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;
• Jointly with ITD, reviewing documentation for PCI compliance certification;
• Jointly with ITD, approving any POS device or system to be used within MDC;
• Working together with ITD to engage the services of a PCI QSA, in consultation with the County Attorney’s Office and Internal Services 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;
• Jointly with ITD, working with the QSA during the compliance review process to provide documentation, 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 Deputy Mayor/Finance Director;
• Maintaining an updated listing of all departments that process credit card transactions using an approved merchant account;
• Conducting annual/bi-annual on-site visits to review processes and assists 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.

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 vulnerability assessment, technology review, risk assessment, compliance assessment and network segmentation services;
• 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;
• Providing incident response and investigation services for security events impacting the cardholder data environment and;
• Monitoring and reviewing computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data;
• Annually complete internal and external penetration testing;
• Bi-annually complete segmentation penetration testing;
• Semi-annually complete internal and external scans. Results are sent to merchant processor;
• Annually update secure build standards and risk assessment;
• Provide online payment application development services:
  o 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. Bi-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/pciincred. The PCI Core Team (members from ITD and Finance) will review the incident response report. A member of the PCI Core Team will respond to the departmental PCI Liaison with appropriate instructions in accordance with MDC’s PCI DSS Incident Response Plan found in the PCI Sharepoint. In addition, refer to the Incident Response Plan for further instructions.

XII. Third Party Vendor Risk Management

Before Purchasing executes an agreement with a payment application vendor, 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 the Internal Services Department’s Purchasing Division to initiate this process.
XIII. Annual Review

This policy will be reviewed on an annual basis in accordance with the PCI Standard. 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

A. Refer to County Policy # 333 regarding applicable procedures for credit card acceptance and processing.

XV. Contract Language for Credit Card Payment Systems

A. Refer to County procedure # 333, Credit Card Acceptance and Processing Procedures, Section V., for requirements applicable to all third-party payment vendor systems.
XVI. PCI Project Calendar

JANUARY

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

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

- Department update of PCI documentation required;
  - Credit Card Procedures (SOPs)
  - PCI Compliance from 3rd party payment vendors
  - Updated Technical and Card Flow Diagrams
  - MID Listing
  - Inventory Report

- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- ITD and Aviation 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 11.2.1 and 11.2.2.

- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly 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 12.11. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- Finance Compliance section 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.

- Departments deadline to complete PCI online course.
- Departments to submit their PCI device inventory into the central location semi-annually.
- PCI Core Team members (ITD & Finance) meet bi-weekly.
- PCI Core Team and senior management quarterly meeting updates.

**FEBRUARY**

- Finance’s Compliance section to create a report of departmental 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 SharePoint.
- ITD completes patch management updates on all system components and software.
- ITD to conduct Risk Assessment Analysis of cardholder data environment.
- PCI Core Team members (ITD & Finance) meet bi-weekly.

**MARCH**

- Finance Compliance section to create a Vendor Management listing and file with copies of all third-party vendor applications PCI compliance documents and upload to SharePoint. (Include Compensating Controls, if required).
- ITD completes patch management updates on all system components and software.
- PCI Core Team members (ITD & Finance) meet weekly.
- Jointly, Finance and ITD to begin working on annual AOC process with QSA.

**APRIL**

- Departmental onsite visits with QSA are scheduled.
- Continue Attestation process.
• ITD conducts bi-annual Penetration Testing.

• ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

• ITD and Aviation 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 11.2.1 and 11.2.2.

• ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly 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 12.11. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

• ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

• PCI Core Team members (ITD & Finance) meet weekly.

• PCI Core Team and senior management quarterly meeting updates.

**MAY**

• Continue Attestation and Departmental on-site visits by QSA.

• Finance Compliance section to obtain drafts of SAQs from QSA and send to Departments for review and approval by PCI Liaisons.

• Finance Compliance section to obtain final SAQs and Attestation documents for review and final signatures by Department Directors.

• ITD completes patch management updates on all system components and software.

• PCI Core Team members (ITD & Finance) meet weekly.
JUNE

- Finance Compliance section to obtain final approved forms from Departments.
- Obtain final approval on submittal SAQs and Attestation from Deputy Mayor.
- Submission deadline for PCI compliance, submit final forms to Merchant providers.
- Departments to submit their PCI device inventory into the central location semi-annually.
- ITD completes patch management updates on all system components and software.
- PCI Core Team members (ITD & Finance) meet weekly.

JULY

- Post-compliance review meeting with QSA, senior management, and PCI Core Team
- Begin work on follow-up items.
- Procedural on-site visits conducted by Finance.
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD and Aviation 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 11.2.1 and 11.2.2.
- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly 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 12.11. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI
requirement 11.1. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- PCI Core Team and senior management quarterly meeting updates.

**AUGUST**

- Post Audit work.
- Procedural on-site visits conducted by Finance Compliance section.
- ITD completes patch management updates on all system components and software.

**SEPTEMBER**

- Procedural on-site visits conducted by Finance.
- Post Audit work.
- ITD completes patch management updates on all system components and software.
- Quarterly sign-off sheet to be provided.

**OCTOBER**

- Post Audit work.
- Procedural on-site visits conducted by Finance Compliance section.
- Bi-Annual Penetration Test.
- ITD completes quarterly review of monthly patch management for all system components and software application to credit card environment, as per PCI requirement 6.2. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.
- ITD and Aviation 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 11.2.1 and 11.2.2.
- ITD completes quarterly anti-virus review, as per PCI requirement 5.2. Quarterly 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 12.11.
Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- ITD completed quarterly testing for Wireless Wardriving to detect and identify all authorized and unauthorized wireless access points, as per PCI requirement 11.1. Quarterly sign-off sheet with results is provided to ITD’s PCI Liaison and uploaded into the central location.

- PCI Core Team to update PCI on-line training course to include new changes

- PCI Core Team and senior management quarterly meeting updates.

**NOVEMBER/DECEMBER**

- ITD to update and complete configuration standards.

- PCI Core Team to finalize PCI On-line training course to include new changes.

- PCI Core Team to prepare PCI annual presentation.

- 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 Compliance section.

- ITD completes patch management updates on all system components and software.