Murphy-Hoffman Company

PCI Architecture Workshop

Version 1.0

September 30, 2017

# Version Control

|  |  |
| --- | --- |
| PCI DSS GAP Assessment | |
| Client Name | Murphy-Hoffman Company |
| Client Contact | Eddie Zuniga, PMO Manager |
| Document Issue No | 1.0 |
| Author(s) | Kylen Griffin – Governance, Risk & Compliance |
| Reviewed by: | Keith Knerr – PCI QSA |
| Project Manager | Alexis Hayob – Project Manager |
| Delivery Date | September 30, 2017 |
| Data Classification | Client Confidential |

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History | | | |
| Version | Description | Author | Date |
| 1.0 | Initial Version | Kylen Griffin | September 30, 2017 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Version Control 2](#_Toc494704074)

[Executive Summary 4](#_Toc494704075)

[Background 4](#_Toc494704076)

[Goals & Objectives 4](#_Toc494704077)

[Security Program Analysis 5](#_Toc494704078)

[Gap Assessment Methodology 5](#_Toc494704079)

[Gap Assessment Scorecard 5](#_Toc494704080)

[Findings and Recommendations 7](#_Toc494704081)

[Initiatives 7](#_Toc494704082)

[01 - Hardening Guides 7](#_Toc494704083)

[02 - Update Network Diagrams and Configurations 7](#_Toc494704084)

[03 - Logging and Monitoring Program 7](#_Toc494704085)

[04 - Incident Response 8](#_Toc494704086)

[05 - Vulnerability Management 8](#_Toc494704087)

[06 - Risk Management 9](#_Toc494704088)

[07 - Penetration Testing 10](#_Toc494704089)

[08 - Policy and Procedure Development 10](#_Toc494704090)

[09 - Vendor Management 10](#_Toc494704091)

[10 - Tablet Plan 11](#_Toc494704092)

[11 - Remote Desktop Plan 12](#_Toc494704093)

[12 - Tamper Proof Plan 12](#_Toc494704094)

[13 - Change Control 13](#_Toc494704095)

[Executive Roadmap 15](#_Toc494704096)

[Conclusion 16](#_Toc494704097)

[Appendix I 17](#_Toc494704098)

[Control Rating Definitions 17](#_Toc494704099)

[Appendix II 18](#_Toc494704100)

[MHC PCI Gap Requirement Ratings 18](#_Toc494704101)

# Executive Summary

## Background

Murphy-Hoffman Company (“MHC”) has requested assistance with evaluating and improving the company’s current information security program. Working directly with MHC, Fishtech Group (“Fishtech”) executed a Payment Card Industry Data Security Standard gap assessment (“PCI DSS”). The assessment reviewed the current information security approach from both the technology and program aspect to ensure MHC is maximizing the current investment in resources to protect company information assets. The assessment will allow MHC to more closely align with the PCI DSS benchmark and further mature the MHC security program.

## Goals & Objectives

The outcome of the gap assessment is to identify areas where MHC may have opportunities for improvement from a security perspective as well as identify areas where MHC could increase operational efficiencies and lower operating costs without compromising security controls. The assessment will identify areas that MHC is doing well. Additionally, the assessment will:

* Provide a foundation to build and mature the information security program
* Provide a framework and leading practice approach against which to continually compare the existing information security program
* Assess MHC’s information security program against the PCI DSS benchmark

# Security Program Analysis

## Gap Assessment Methodology

Fishtech evaluated the organization’s current implementation of its information security program against PCI DSS 3.2 benchmark. As part of the assessment, Fishtech conducted a high-level network security architecture and policy review. Based on these reviews, Fishtech will provide a security roadmap of initiatives that will enable MHC to enhance its information security program. Fishtech will have a current PCI-DSS Qualified Security Assessor (“QSA”) that will provide validation and technical peer review of the gap analysis documentation. Additionally, the QSA will be available for any questions or clarification during the assessment.

Fishtech’s methodology for this assessment employed a practical methodology that analyzes current technologies, policies, processes, and activities to determine how current operations are meeting MHC’s stated requirements and objectives.

The methodology begins with understanding MHC’s operating model, culture, and stated goals. Fishtech’s assessment team will interview key stakeholders to ensure we have an appreciation for MHC’s current and future initiatives. It is crucial for us to understand areas of concern/interest in order to provide the most appropriate recommendations. Fishtech’s methodology is to assist organizations with building effective and efficient security program.

Our consultants will rely on both expert analysis and common sense when evaluating MHC’s security program. Throughout the entire review, MHC’s business requirements will be the driving force behind every recommendation developed and presented. A project of this nature is a cooperative endeavor, and it is the sole goal to serve MHC’s best interests.

Fishtech’s methodology is to work in a collaborative manner to be sure there is proper knowledge transfer during the engagement. This will allow MHC’s information security team to effectively address any findings and recommendations once the assessment has concluded.

## Gap Assessment Scorecard

Fishtech developed the Gap Assessment Scorecard for MHC by reviewing the documentation provided and interviewing key MHC personnel. The review compared existing and future MHC projects and documentation against PCI DSS 3.2 standard. During the engagement, Fishtech identified deficiencies with MHC’s security program. The breakdown of controls included the following:

Figure 1: PCI DSS Control Category Summary

# Findings and Recommendations

## Initiatives

### 01 - Hardening Guides

MHC should create hardening guides that are based on best practices from Center for Internet Security (“CIS”), National Institute of Standards and Technology (“NIST”), and SANS Institute. These guides and benchmarks should be validated in a lab environment to ensure that none of the critical business functions that MHC employs are disrupted by these changes.

All computers that touch the PCI environment should be hardened or secured to reduce the services running and vulnerabilities on that system. This initiative supports the PCI DSS Requirement 2.2, and must be undertaken if the remote desktop plan is utilized.

### 02 - Update Network Diagrams and Configurations

MHC should establish procedures to ensure that all updates to the network design are accurately captured and published. Currently, MHC is undergoing a major change to their environment as they are rolling out the tablets to their branches. As MHC performs these and future updates, both external and internal data flows, security devices, communication paths, and network design should be captured accurately into the published network design documentation.

### 03 - Logging and Monitoring Program

MHC has basic audit log functions enabled in their information system enterprise. These audit logs not being collected and are kept on the devices. These logs can be monitored although no analysis is being performed on these logs at the time of the assessment. It is recommended that MHC develop Logging and Monitoring Policy and Procedures to establish an Audit Log program within the organization that includes:

* Develop baseline activity profiles for systems within the monitoring and centralized logging system scope
* Develop an automated mechanism to collect and aggregate all logs to a centralized location
* Develop a review plan to ensure that all of the following are looked at daily
  + All Security Events
  + Logs of all system components that store, process, or transmit card holder data and/or sensitive authentication data
  + Logs of all critical system components
  + Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).
* Develop thresholds that include the following:
  + Access of individuals to sensitive data
  + Privileged account access to data
  + Individual access to audit trail data and functions
  + Invalid logical access attempts
  + Identification and authentication actions
  + Initialization of auditing and ensuring integrity of the audit logs
  + Creation and deletion of system-level objects.
  + Alerts appropriate staff members of questionable activity
* Collaborate with external parties to develop alerting capabilities and perform ongoing tuning of thresholds and alerts

### 04 - Incident Response

While basis IT recovery procedures are in place, MHC should establish IT incident management procedures that are specific to physical and information security incidents. It is recommended that MHC establish a formal security incident management program with documented policies and procedures that follow best practices.

The policies and procedures should incorporate the following key elements for security incidents:

* Organization is defined with a central point of contact, defined roles, and titles
* The Incident Response team roster is maintained identified with names and telephone numbers of incident response team members.
* Response team availability is documented
* Timelines for incident detection and disclosure are documented where timelines are defined for each severity level
* Management of evidence (i.e., identification, collection, transfer, and preservation) for the purposes of disciplinary and legal action
* Escalation procedures to engage key personnel (i.e., management, legal, and HR) and third-parties (i.e., law enforcement)
* Containment activities
* Security incident process lifecycle is defined including the following:
  + Identification of security incident
  + Assignment of severity to each security incident
  + Development of responses
  + Identification of resolution
  + Monitoring with reporting
* After incident activities should be documented and utilized as lessons learned to further strengthen the Incident Response Plan.
* Additional tabletop exercises should be utilized to ensure that all Incident Response team members understand and can execute their role within the plan.

In addition, MHC should also come up with a mechanism to have their legal department keep in touch with the ever-changing landscape of data breach notification at the state level. Most states that MHC has business in has some sort of data breach notification statue in place. These should be reviewed at least semiannually for changes since legislative issues at each state could impact this information.

### 05 - Vulnerability Management

It is recommended that MHC develop vulnerability management policies and procedures. As a minimum, patch management policies and procedures should be written to address the following key elements:

* Roles and responsibilities for vulnerability scanning and patch management
* Complete asset management to determine IT assets (servers, workstations, network devices, mobile devices, etc.) in use
* Scan all IT assets for vulnerabilities and feeding that information into the patch management program
* Monitoring sources of information about patches
* Assessing risks and prioritizing patches
* Controls over testing, distribution, and deployment, including automatic deployment
* Managing information about patches
* Ongoing scanning
* Documenting an exception process

MHC should also conduct regular scans for unauthorized software on the network and establish procedures with tools to conduct application security scans to ensure all scans and remediation efforts are auditable. All scan should be done by trained qualified personal, and should be done internally at least quarterly with remediation taking place and rescans completed until passing scans are achieved. External vulnerability scanning should be performed as well quarterly by an PCI DSS Approved Scanning Vendor with rescans done until a passing scan is achieved.

In the future if MHC does start utilizing web applications then special attention should be given to these web applications developed in-house or by third-parties. Applications vulnerability scans should verify the following vulnerabilities:

1. Cross-Site Scripting (“XSS”)

2. Injection flaws, particularly structured query language (“SQL”) injection

3. Malicious file execution; insecure direct object references

4. Cross-Site Request Forgery (“CSFR”)

5. Information leakage and improper error handling

6. Broken authentication and session management

7. Insecure cryptographic storage

8. Insecure communications

9. Failure to restrict uniform resource locator (“URL”) access

For best practice recommendations consideration should be given to the following resource: NIST SP800-40 Revision3, Guide to Enterprise Patch Management Technologies.

### 06 - Risk Management

Risk management policies and procedures are not documented. MHC’ risk profile and risk tolerance are not well-defined and managed. Without this knowledge, it will be difficult for MHC to make effective business decisions about information security and allocate resources (i.e. time and money) efficiently.

It is recommended that MHC develop a risk management program with policies, procedures and standards. MHC should take steps to develop a risk management process to identify and evaluate IT risks within the context of the overall business and its enterprise. The risk management process should facilitate the identification, quantification, and prioritization of IT risks with respect to critical business processes objectives and MHC’ risk tolerance (risk acceptance levels). More specifically it is recommended that MHC develop a formal risk management program that is closely aligned with the business enterprise.

The risk management program should revolve around a methodology that identifies the following key elements:

* Business assets including critical business processes and services (refer to ST04: Disaster Recovery/Contingency Planning)
* IT infrastructure including critical IT processes and services
* Range of threats to critical business processes and services
* MHC’ business processes, services, assets and threats and analysis of associated risks
* MHC’ IT processes and services and threats and evaluation of associated risks
* Interrelationships (dependency analysis) between business processes and services, IT processes and services and physical IT assets
* Scenarios (scenario analysis) with vulnerability assessments for each threat-asset (process, services, physical asset) combination
* Process to capture business changes in addition to IT changes for risks analysis
* Integration with other key IT processes such as change management, audits, asset management and vulnerability management, among others
* Response to risks including preventive, detective, corrective and predictive
* Actions to mitigate risks (risk treatment plan) that include descriptions of options to accept, avoid, transfer and insure the risk

Consideration should be given to the following resources: NIST 800-30 Revision 1 Risk Management Guide for Information Technology Systems and NIST 800-37 Revision 1 Guide for Applying the Risk Management Framework.

### 07 - Penetration Testing

MHC should establish procedures to conduct and manage regular penetration tests and track remediation activities. These procedures should be utilized for all outside parties that are performing the penetration testing. The methodology that should be utilized for this penetration testing procedure are as follows:

* Based on industry-accepted penetration testing approaches (for example, NIST SP800-115 “Technical Guide to Information Security Testing and Assessment”)
* Includes coverage for the entire card holder data environment perimeter and critical systems
* Includes testing from both inside and outside the network
* Includes testing to validate any segmentation and scope-reduction controls
* Defines application-layer penetration tests to include, at a minimum, the application vulnerabilities listed in Initiative 05 – Vulnerability Management of this document and Requirement 6.5 of the PCI DSS.
* Defines network-layer penetration tests to include components that support network functions as well as operating systems
* Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
* Specifies retention of penetration testing results and remediation activities results.
* Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

### 08 - Policy and Procedure Development

Developing information security policies that set the security tone and direction for MHC is a major area for improvement. Information security policies, procedures, and standards are not fully documented for all of the requirement families within PCI DSS. It is recommended that MHC develop detailed policies for major information security areas, and then create supporting standards for that area. Developing a comprehensive set of governing policies and standards is an excellent start to building a foundation of the corporate information security program.

This initiative can be complex and resource intensive. To begin, it is recommended that MHC focus on one policy at a time until all policies are addressed. It is intended to bring order to subsequent policy initiatives and set the security tone for IT and the other parts of the business. This approach also provides MHC with a basic set of policies in a short period.

Additional resources for expanding this program: NIST SP800-18 Revision 1, “Developing Security Plans”, and NIST SP800-53 “Security and Privacy Controls”.

### 09 - Vendor Management

This program is focused on leveraging tools and processes to ensure due diligence has been completed and is maintained with third-party organizations that supply vital resources. It will include tracking, interviewing, and assessing third-party security processes and technology. Although the IT controls are in scope here, a more comprehensive approach of incorporating all corporate requirements related to third-party partnerships may be evaluated and tracked within this strategic effort.

During the interview process, Fishtech discovered that MHC lacks some key elements found in a mature vendor/business partner management program. Proper oversight of key business partners should be an integral part of an overall enterprise risk management program, especially in today’s business climate where there is growing incentive to migrate data to hosted environments or outsource operational functions.

Fishtech recognizes vendors vary dramatically based by region / business unit / vendor function; however, the due diligence process should be streamlined. It is critical that the Information Security department be informed when new vendor relationships are engaged in order to perform the appropriate level of security due diligence on that vendor and formally document the risks in doing business with that particular vendor.

* To understand the breadth of what this project may entail, it is recommended to begin with small achievements first and evolve the program over time. Some recommended areas to begin developing this program are:
  + First, the primary teams responsible for managing vendor relationships (e.g. IT, Legal, and compliance) should collaborate with the Procurement Team, who’s responsible for maintaining the list of all vendor relationships
  + Second, develop a Business Partner Assessment (“BPA”) Policy and Standard (and achieve management buy-in)
  + Next, create a “Vendor Categorization Model” – At first MHC should work to categorize its business partner relationships based on risk qualifiers, such as:
    - How the data is accessed and stored, transmitted, regulatory requirements, and dependency on their service
* Lastly, socialize the new assessment procedure with key business units to inform and educate them of the new required process.

A common pitfall to developing an enterprise-wide BPA is not properly socializing the business need and importance. In addition, BPA programs may fall short due to a lack of education on the process. If business units view this program as a roadblock—they may attempt to circumvent the process. As MHC assesses the approach for implementing a new BPA program, it is important to be aware of this potential pitfall to minimize any impact to the corporate culture.

### 10 - Tablet Plan

Further discussions were held to find an architecture design that would keep the PCI scope as small as possible. It was discovered through the workshop that Curbstone had a reference architecture that utilized tablets to enter the credit card data instead of the computer. This design would keep the computer out of PCI DSS scope and would allow for the easiest path toward complete PCI DSS compliance. This option would include only the costs of the mobile device management license and the tablet, and configuring separate wireless VLANs.

The PCI DSS reporting requirements for this option would be for the systems in scope, which would be the tablets and any network devices those tablets touch. SAQ C V/T is a self-assessment questionnaire that covers the following PCI DSS requirements:

* Requirement 1: Install and maintain a firewall configuration to protect data
* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
* Requirement 3: Protect stored cardholder data
* Requirement 4: Encrypt transmission of cardholder data across open, public networks
* Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
* Requirement 6: Develop and maintain secure systems and applications
* Requirement 7: Restrict access to cardholder data by business need to know
* Requirement 9: Restrict physical access to cardholder data
* Requirement 12: Maintain a policy that addresses information security for all personnel

### 11 - Remote Desktop Plan

During the PCI Workshop, MHC and Fishtech discussed the proposed architecture designs for the MHC project. This design uses the PC to input credit card information through a RDP Sessions, a Forward Proxy, and finally an iFrame. It was concluded that the RDP session would be the best answer out of these three. But this proposed architecture design would have placed the entire computer under scope for PCI DSS. This option cost would include the cost of the RDP license in addition to the configuration of virtual LANs (“VLANs”) throughout the enterprise to keep the computers at the locations as segregated as possible.

This option would take the longest to completely implement since it would require for all of the computers that process the credit card information a full SAQ D, which is the self-assessment questionnaire D that contains the entire PCI DSS standard. Because all of the computer would be in scope, the amount of work that would be involved would be extensive. This would require items listed in the SAQ C V/T below in addition to computer hardening, logging and monitoring, quarterly vulnerability scans, annual penetration tests, as well as other items. The following PCI DSS requirements make up the SAQ D.

* Requirement 1: Install and maintain a firewall configuration to protect data
* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
* Requirement 3: Protect stored cardholder data
* Requirement 4: Encrypt transmission of cardholder data across open, public networks
* Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
* Requirement 6: Develop and maintain secure systems and applications
* Requirement 7: Restrict access to cardholder data by business need to know
* Requirement 8: Identify and authenticate access to system components
* Requirement 9: Restrict physical access to cardholder data
* Requirement 10: Track and monitor all access to network resources and cardholder data
* Requirement 11: Regularly test security systems and processes
* Requirement 12: Maintain a policy that addresses information security for all personnel

### 12 - Tamper Proof Plan

MHC should implement tampering procedure for the tablets to ensure that they have not been tampered with or their configuration changed from the approved standard. Items to include in the plan are as follows:

* Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
* Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).
* Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:
  + Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
  + Do not install, replace, or return devices without verification.
  + Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
  + Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

### 13 - Change Control

While basic change control procedures are in place for systems, network devices, and applications, formal policies and procedures are not documented. MHC should develop audit trails for all change management policies and procedures. Change logs, meeting minutes, remediation activities are all ways MHC can achieve this auditable state.

MHC’s information resources (i.e., networks, applications, systems, etc.) should be governed by formal documented change control procedures to ensure that only authorized changes are committed to production. It is recommended that MHC document formal change management policies and procedures.

The policies and procedures should include the following key elements:

* Identification and recording of significant changes
* Planning and testing of changes
* Assessment of the potential impacts, including security impacts, of such changes
* Formal approval procedure for proposed changes from application, system, or business owners
* Communication of change details to all relevant persons
* Fallback procedures
* Enforcement
* Audit trail of changes
* Configuration management and version control of all software updates
* Notification of unauthorized modification of critical system or content files

It is also recommended that MHC develop a formal process to document changes to applications, operating systems, and its network enterprise. All change control documentation should reflect an audit trail of the change, including the date and time of change, reason for change, the name of the person making the change, and the person or persons who authorized the change. Changes to operating system modules, tables, libraries, application software, networks, etc., should become a permanent part of the system, operations, or network documentation. MHC currently is performing a highly auditable procedure with the inclusion of JIRA as its application project and issue tracker. Additional procedures and standards should be created to ensure that this process is well documented and formalized for MHC with a complete audit trail. Key elements to be documented for the audit trail should include:

* Person making the change; the time and date of change
* Business justification for the change and nature of defect (if applicable)
* Estimated resource requirements necessary to complete the change
* Testing required
* Back-out procedures
* Systems impacted
* User contact information

| Ref# | Recommendation | Priority | Timeframe | Resource | Investment | Product Component |
| --- | --- | --- | --- | --- | --- | --- |
| 01 | Hardening Guides | MEDIUM | 15-18 months | Internal  1-2 FTE | $ | Possible |
| 02 | Update Network Diagrams and Configurations | HIGH | 3-6 months | Internal  1-2 FTE | $ | No |
| 03 | Logging and Monitoring Program | HIGH | 9-12 month | Blended  2-3 FTE | $$ | Yes |
| 04 | Incident Response | MEDIUM | 9-12 month | Internal  1-2 FTE | $ | Yes |
| 05 | Vulnerability Management | MEDIUM | 6-9 months | Internal  1-2 FTE | $$ | Yes |
| 06 | Risk Management | MEDIUM | 3-6 months | Blended  1-2 FTE | $ | Possible |
| 07 | Penetration Testing | MEDIUM | 1-3 months | External | $ | No |
| 08 | Policy and Procedure Development | HIGH | 6-9 months | Internal/Blended  1-2 FTE | $ | No |
| 09 | Vendor Management | LOW | 1-3 months | Blended  1 FTE | $ | No |
| 10 | Tablet Plan | HIGH | 3-6 months | Internal  1-2 FTE | $$ | Yes |
| 11 | Remote Desktop Plan | LOW | 18-24 months | Internal  2-3 FTE | $$ | Yes |
| 12 | Tamper Proof Plan | MEDIUM | 3-6 months | Internal  1 FTE | $ | Possible |
| 13 | Change Control | MEDIUM | 6-9 months | Internal  1 FTE | $ | Possible |

**\*Investment**

The total investment costs associated with each of the tactical initiatives are estimated based on MHC’s environment, organization, and personnel, as well as typical tool costs and expected level of effort. The following table describes the general ranges of investment costs.

|  |  |
| --- | --- |
| Investment Symbol | Investment Range |
| $ | Up to $40,000 |
| $$ | $40,000 - $100,000 |
| $$$ | $100,000 or more |

## Executive Roadmap

The security roadmap timeline is provided to assist MHC in determining the order in which the initiatives should be undertaken. The timeline can be accelerated or extended to meet business objectives, depending on resource availability, funding, and business conditions. Fishtech recommends that all of the initiatives listed below be reviewed, if not implemented, by the beginning of each budget planning cycle. By conducting this review at the beginning of each budget planning cycle, MHC can reaffirm that the information assurance and business climate still necessitate the implementation of the initiatives.

# Conclusion

Fishtech provided MHC with several recommendations to improve its security program and posture. MHC should act on these recommendations as possible and begin further development of security policies and procedures. The security policies are essential as MHC implements additional technology controls (IDS/IPS, content filtering, etc.) within the network infrastructure. The policies dictate how the technologies need to be configured and where they need to be implemented.

These recommendations will become more mandatory if the switch is made to revert from the tablet plan to the remote desktop plan that was discussed during the PCI Workshop. So, it is advised that the recommendations should be considered during the next fiscal year planning. Fishtech can assist MHC with implementing the identified recommendations and in remediating any of the identified security risks. Fishtech can also assist MHC in identifying the most appropriate security technologies within MHC’s network architecture.

Overall, MHC’s security program and architecture is maturing and developing as needed. The Information Technology department is limited by the number of resources that can contribute to information security. While there are some challenges facing MHC, the emphasis from senior management and workforce members on security is making an impact. Everyone at MHC was receptive of this engagement and vowed to enact the recommendations where the business case supports the effort. Policy development, logging/monitoring and incident response are the long-term goals of MHC. These initiatives will greatly enhance the security of the program for the foreseeable future.

Several of the security threats identified can cause serious harm to the MHC business operations if they are not corrected. Numerous security controls are in place and configured securely. However, as the organization grows from an employee and network standpoint, additional security controls need to be implemented to properly protect MHC’s IT architecture, assets, and data.

In conclusion, Fishtech believes that by implementing the recommendations outlined in this report, MHC will not only improve the security posture of the organization, but also help establish the program as a strategic part of overall corporate governance. The roadmap should be revisited quarterly to ensure that it remains practical and adequate to meet the needs of the business. Fishtech is confident that by establishing a solid governance foundation for the information security program, MHC will properly align its projects, policies, and technology acquisitions with clear business objectives and priorities.

# Appendix I

## Control Rating Definitions

* **Absent** – No existing policy, procedure, or standard was identified that would fully satisfy the requirements of industry regarded security best practices or applicable regulatory mandates.
* **Implemented** – Sufficient policies, procedures, or standards exist to satisfy the requirements of industry regarded security best practices or applicable regulatory mandates.
* **In Progress** –Existing policy, procedure, or standard was identified that would partially satisfy the requirements of industry regarded security best practices or applicable regulatory mandates. However, additional actions are being taken to fully satisfy these requirements.
* **Not Applicable** – Control was not applicable to the assessed framework.

# Appendix II

## MHC PCI Gap Requirement Ratings

| PCI DSS Requirement | Requirement Statement | Observations | Requirement Rating | Initiative |
| --- | --- | --- | --- | --- |
| *Requirement 1: Install and maintain a firewall configuration to protect cardholder data* | | | | |
| 1.1.0 | Establish and implement firewall and router configuration standards that include the following: | Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. Additional configurations would need to be implemented for the PC plan. The configurations are there and just had to be replicated and verified when all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.1.1 | A formal process for approving and testing all network connections and changes to the firewall and router configurations | Changes are submitted through JIRA and are reviewed by the Change Advisory Board or Director of IT. All of the participants on the change are named and any found non-compliance is a learning experience. MHC should document this process and ensure that all network administrators follow it. | In Progress | 08 - Policy and Procedure Development |
| 1.1.2 | Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks | Diagrams would have to be updated to reflect the wireless access for the plans. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.1.3 | Current diagram that shows all cardholder data flows across systems and networks | Existing diagrams will have to be updated to reflect this information | In Progress | 02 - Update Network Diagram and Configurations |
| 1.1.4 | Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | MHC does not utilize a DMZ since from their tablet solution it's only establishing a connection to the approved gateway. The only inbound traffic is the established outbound connection to the gateway. | Not Applicable | 10 - Tablet Plan |
| 1.1.5 | Description of groups, roles, and responsibilities for management of network components | Every user has a unique username within the networking environment. Written documentation should be updated to reflect these roles and responsibilities. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.1.6 | Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. | Documentation will need to be addressed to provide the business justification for the C2 gateway, tablet, and tablet management communications. | In Progress | 08 - Policy and Procedure Development |
| 1.1.7 | Requirement to review firewall and router rule sets at least every six months | Technology is in place to achieve this requirement and the documentation is being drafted to address this procedure. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.2.0 | Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. | Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. Additional configurations would need to be implemented for the PC plan. The configurations are there and just had to be replicated and verified when all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.2.1 | Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. | Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. Additional configurations would need to be implemented for the PC plan. The configurations are there and just had to be replicated and verified when all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.2.2 | Secure and synchronize router configuration files. | Technology is in place to achieve this requirement, just need to validate once all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.2.3 | Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. | Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. Additional configurations would need to be implemented for the PC plan. The configurations are there and just had to be replicated and verified when all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.3.0 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. Additional configurations would need to be implemented for the PC plan. The configurations are there and just had to be replicated and verified when all of the branches are rolled out. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.3.1 | Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | MHC is utilizing the virtual wire technology from Palo Alto with policies to limited inbound and outbound traffic to just those that the solution needs to communicate. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.3.2 | Limit inbound Internet traffic to IP addresses within the DMZ. | MHC does not utilize a DMZ since from their tablet solution it's only establishing a connection to the approved gateway. The only inbound traffic is the established outbound connection to the gateway. | Not Applicable | 10 - Tablet Plan |
| 1.3.3 | Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.) | For the MHC PCI network that is in scope, the only traffic they allow from the internet is to the processing gateway from Curbstone. | In Progress | 02 - Update Network Diagram and Configurations |
| 1.3.4 | Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | All outbound traffic from the PCI network are to the approved gateway. | in Progress | 02 - Update Network Diagram and Configurations |
| 1.3.5 | Permit only “established” connections into the network. | All outbound traffic from the PCI network are to the approved gateway. | in Progress | 02 - Update Network Diagram and Configurations |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | None |
| 1.3.7 | Do not disclose private IP addresses and routing information to unauthorized parties. | MHC is utilizing methods to mask the private IP address and routing information. | Implemented | None |
| 1.4.0 | Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:  · Specific configuration settings are defined.  · Personal firewall (or equivalent functionality) is actively running.  · Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices | MHC PCI environment does not contain any devices that could have a personal firewall installed. They are using a mobile device management solution to manage the tablets. | Not Applicable | None |
| 1.5.0 | Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters* | | | | |
| 2.1.0 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). | MHC removes all of the default vendor provided password for their equipment. If MHC can, they will disable the account if it's not necessary | Implemented | None |
| 2.1.1 | For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | MHC removes all of the default vendor provided password and other configurations elements for their equipment. | Implemented | None |
| 2.2.0 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: · Center for Internet Security (CIS) · International Organization for Standardization (ISO) · SysAdmin Audit Network Security (SANS) Institute · National Institute of Standards Technology (NIST). | MHC does not maintain any hardening guides for their environment | Absent | 01 - Hardening Guides |
| 2.2.1 | Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.2.3 | Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.2.4 | Configure system security parameters to prevent misuse. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.2.5 | Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.3.0 | Encrypt all non-console administrative access using strong cryptography. | MHC PCI environment does not contain any consoles at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 2.4.0 | Maintain an inventory of system components that are in scope for PCI DSS. | MHC through the mobile device management software does keep an inventory of the Android tablets that are within their PCI environment | Implemented | 10 - Tablet Plan |
| 2.5.0 | Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 2.6.0 | Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.* | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| *Requirement 3: Protect stored cardholder data* | | | | |
| 3.1.0 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: · Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements · Specific retention requirements for cardholder data · Processes for secure deletion of data when no longer needed · A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 3.2.0 | Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.2.1 | Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.2.2 | Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not- present transactions) after authorization. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.2.3 | Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.3.0 | Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.4.0 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: · One-way hashes based on strong cryptography, (hash must be of the entire PAN) · Truncation (hashing cannot be used to replace the truncated segment of PAN) · Index tokens and pads (pads must be securely stored) · Strong cryptography with associated key-management processes and procedures | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. All MHC receives from Curbstone's gateway is a token for the transaction. | Not Applicable | 10 - Tablet Plan |
| 3.4.1 | If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. | MHC is currently not utilizing any storage level encryption on the Android tablets that are in their PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.5.0 | Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 3.5.1 | Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: · Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date · Description of the key usage for each key · Inventory of any HSMs and other SCDs used for key management | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 3.5.2 | Restrict access to cryptographic keys to the fewest number of custodians necessary. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.5.3 | Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: · Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key · Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) · As at least two full-length key components or key shares, in accordance with an industry- accepted method | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 3.5.4 | Store cryptographic keys in the fewest possible locations. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.0 | Fully document and implement all key- management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.1 | Generation of strong cryptographic keys | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.2 | Secure cryptographic key distribution | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.3 | Secure cryptographic key storage | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.4 | Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.5 | Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.6 | If manual clear-text cryptographic key-management operations are used, these operations musts be managed using split knowledge and dual control. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.7 | Prevention of unauthorized substitution of cryptographic keys. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.6.8 | Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key- custodian responsibilities. | MHC PCI environment does not contain any servers at this time. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 10 - Tablet Plan |
| 3.7.0 | Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| *Requirement 4: Encrypt transmission of cardholder data across open, public networks* | | | | |
| 4.1.0 | Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: · Only trusted keys and certificates are accepted. · The protocol in use only supports secure versions or configurations. · The encryption strength is appropriate for the encryption methodology in use. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 4.1.1 | Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. | MHC is utilizing WPA2 for the tablet plan rollout in their PCI environment. | Implemented | 10 - Tablet Plan |
| 4.2.0 | Never send unprotected PANs by end- user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.). | MHC is locking down the tablets within the PCI environment to kiosk mode only. This will just enable a browser to go to one location, which is the location of the Curbstone gateway. | Implemented | 10 - Tablet Plan |
| 4.3.0 | Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| *Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs* | | | | |
| 5.1.0 | Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | MHC is testing functionality of the mobile device management software to see if anti-virus can be included to the Android tablets. | In Progress | 10 - Tablet Plan |
| 5.1.1 | Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | MHC is testing functionality of the mobile device management software to see if anti-virus can be included to the Android tablets. | In Progress | 10 - Tablet Plan |
| 5.1.2 | For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. | MHC is actively scanning the landscape to determine the malware threats and critical patches that the Android systems will require in the future. | Implemented | 10 - Tablet Plan |
| 5.2.0 | Ensure that all anti-virus mechanisms are maintained as follows: · Are kept current, · Perform periodic scans · Generate audit logs which are retained per PCI DSS Requirement 10.7. | MHC is testing functionality of the mobile device management software to see if anti-virus can be included to the Android tablets. | In Progress | 10 - Tablet Plan |
| 5.3.0 | Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. | MHC is testing functionality of the mobile device management software to see if anti-virus can be included to the Android tablets. | In Progress | 10 - Tablet Plan |
| 5.4.0 | Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| *Requirement 6: Develop and maintain secure systems and applications* | | | | |
| 6.1.0 | Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. | MHC does not have any internal analysis or ranking of vulnerabilities. MHC would rely on the vulnerability scanning tool to determine the criticality level of the vulnerability. MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Not Applicable | 05 - Vulnerability Management |
| 6.2.0 | Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. | In the MHC PCI environment, all patches will be pushed out through the mobile device management software since they are all tablets. Although, MHC does not have any internal analysis or ranking of vulnerabilities, they are patching their workstations every 15th and 23rd of the month via Microsoft SCCM. | Not Applicable | 05 - Vulnerability Management |
| 6.3.0 | Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: · In accordance with PCI DSS (for example, secure authentication and logging) · Based on industry standards and/or best practices. · Incorporating information security throughout the software-development life cycle | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.3.1 | Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.3.2 | Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: · Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. · Code reviews ensure code is developed according to secure coding guidelines · Appropriate corrections are implemented prior to release. · Code-review results are reviewed and approved by management prior to release. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.0 | Follow change control processes and procedures for all changes to system components. The processes must include the following: | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.1 | Separate development/test environments from production environments, and enforce the separation with access controls. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.2 | Separation of duties between development/test and production environments | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.3 | Production data (live PANs) are not used for testing or development | MHC utilizes fake/dummy credit cards for their testing and development environment. MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.4 | Removal of test data and accounts from system components before the system becomes active / goes into production. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.4.5 | Change control procedures must include the following: | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 6.4.5.1 | Documentation of impact. | MHC should review the change control policy that is currently being created to firmly address these control requirements | In Progress | 12 - Change Control Plan |
| 6.4.5.2 | Documented change approval by authorized parties. | MHC should review the change control policy that is currently being created to firmly address these control requirements | In Progress | 12 - Change Control Plan |
| 6.4.5.3 | Functionality testing to verify that the change does not adversely impact the security of the system. | MHC should review the change control policy that is currently being created to firmly address these control requirements | In Progress | 12 - Change Control Plan |
| 6.4.5.4 | Back-out procedures. | MHC should review the change control policy that is currently being created to firmly address these control requirements | In Progress | 12 - Change Control Plan |
| 6.4.6 | Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. | MHC should review the change control policy that is currently being created to firmly address these control requirements | In Progress | 12 - Change Control Plan |
| 6.5.0 | Address common coding vulnerabilities in software-development processes as follows: · Train developers at least annually in up- to-date secure coding techniques, including how to avoid common coding vulnerabilities. · Develop applications based on secure coding guidelines. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.1 | Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.2 | Buffer overflows | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.3 | Insecure cryptographic storage | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.4 | Insecure communications | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.5 | Improper error handling | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.6 | All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.7 | Cross-site scripting (XSS) | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.8 | Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.9 | Cross-site request forgery (CSRF) | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.5.10 | Broken authentication and session management. | MHC PCI environment does not utilize applications with the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 6.6.0 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: · Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes | MHC does not have any public-facing web applications. | Not Applicable | 10 - Tablet Plan |
| 6.7.0 | Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| *Requirement 7: Restrict access to cardholder data by business need to know* | | | | |
| 7.1.0 | Limit access to system components and cardholder data to only those individuals whose job requires such access. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.1.1 | Define access needs for each role, including: · System components and data resources that each role needs to access for their job function · Level of privilege required (for example, user, administrator, etc.) for accessing resources. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.1.3 | Assign access based on individual personnel’s job classification and function. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.1.4 | Require documented approval by authorized parties specifying required privileges. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.2.0 | Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. This access control system(s) must include the following: | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.2.1 | Coverage of all system components | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.2.2 | Assignment of privileges to individuals based on job classification and function. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.2.3 | Default “deny-all” setting. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 7.3.0 | Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| *Requirement 8: Identify and authenticate access to system components* | | | | |
| 8.1.0 | Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows: | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 8.1.1 | Assign all users a unique ID before allowing them to access system components or cardholder data. | MHC utilizes unique IDs for all of their employees and even administrator has a separate account for administrative work. | Implemented | None |
| 8.1.2 | Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | MHC employees must submit a ticket to get their accounts modified. An analyst will ensure that the request is authorized and they have valid business reasons for the request | Implemented | None |
| 8.1.3 | Immediately revoke access for any terminated users. | Once MHC received the termination notice from Human Resources, they will work with them to identify the best course of action for the terminated user. This course of action usually defaults to revoke immediate access, but exceptions can be made based on job function. | Implemented | None |
| 8.1.4 | Remove/disable inactive user accounts within 90 days. | MHC does run scripts to disable users after 90 days of inactivity. | Implemented | None |
| 8.1.5 | Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: · Enabled only during the time period needed and disabled when not in use. · Monitored when in use. | MHC utilizes unique IDs for all of their employees and even administrator has a separate account for administrative work. | Implemented | None |
| 8.1.6 | Limit repeated access attempts by locking out the user ID after not more than six attempts. | MHC does lock out the user after less than six attempts are made trying to login. | Implemented | None |
| 8.1.7 | Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | MHC requires an administrator to enable the user id again once the user id has been disabled. | Implemented | None |
| 8.1.8 | If a session has been idled for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | MHC does lock out screens that have been inactive for 15 minutes, which does require them to re-authenticate in order to use their machine again. For IT personnel, MHC utilizes a 5-minute screen lock period due to the nature of the information on their screens. | Implemented | None |
| 8.2.0 | In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: · Something you know, such as a password or passphrase · Something you have, such as a token device or smart card · Something you are, such as a biometric. | MHC utilizes password for all authentication onto their network. | Implemented | None |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | MHC utilizes Microsoft Kerberos, Active Directory for their authentication credentials. | Implemented | None |
| 8.2.2 | Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | MHC does validate the users’ identity before any account maintenance is performed. | Implemented | None |
| 8.2.3 | Passwords/passphrases must meet the following: · Require a minimum length of at least seven characters. · Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above. | MHC does require at least 8 character passwords with complexity. | Implemented | None |
| 8.2.4 | Change user passwords/passphrases at least once every 90 days. | MHC does require their employees to change their password every 90 days. | Implemented | None |
| 8.2.5 | Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. | MHC does track the last 4 passwords used for the user. | Implemented | None |
| 8.2.6 | Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | MHC does require the employee to change their password when they are issued it for the first time. | Implemented | None |
| 8.3.0 | Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 10 - Tablet Plan |
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 10 - Tablet Plan |
| 8.3.2 | Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity’s network. | MHC does utilize a two factor VPN token to access their network. The VPN token is also suspended after 32 days of inactivity, in which case they will need to request VPN access again. | Implemented | None |
| 8.4.0 | Document and communicate authentication policies and procedures to all users including: · Guidance on selecting strong authentication credentials · Guidance for how users should protect their authentication credentials · Instructions not to reuse previously used passwords · Instructions to change passwords if there is any suspicion the password could be compromised. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 8.5.0 | Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: · Generic user IDs are disabled or removed. · Shared user IDs do not exist for system administration and other critical functions. · Shared and generic user IDs are not used to administer any system components. | MHC does not utilize authentication methods that are listed in this control. | Absent |  |
| 8.5.1 | Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 8.6.0 | Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: · Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. · Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. | MHC does not utilize authentication methods that are listed in this control. | Absent |  |
| 8.7.0 | All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: · All user access to, user queries of, and user actions on databases are through programmatic methods. · Only database administrators have the ability to directly access or query databases. · Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | None |
| 8.8.0 | Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| *Requirement 9: Restrict physical access to cardholder data* | | | | |
| 9.1.0 | Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.1.1 | Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.1.2 | Implement physical and/or logical controls to restrict access to publicly accessible network jacks. | MHC has implemented NAC on all of their ports, if someone does happen to plug a device into an available network jack, then device will be sent to a VLAN for the internet only guest network. | Implemented | None |
| 9..1.3 | Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | MHC has implemented NAC on all of their ports, if someone does happen to plug a device into an available network jack, then device will be sent to a VLAN for the internet only guest network. | Implemented | None |
| 9.2.0 | Develop procedures to easily distinguish between onsite personnel and visitors, to include: · Identifying onsite personnel and visitors (for example, assigning badges) · Changes to access requirements · Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.3.0 | Control physical access for onsite personnel to sensitive areas as follows: · Access must be authorized and based on individual job function. · Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.4.0 | Implement procedures to identify and authorize visitors. Procedures should include the following: | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.4.1 | Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.4.2 | Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.4.3 | Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.4.4 | A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law. | MHC has implemented procedures to implement this requirement in their data center, but not in the retail store environments. These requirements would not be feasible since the individuals that visit the store are customers. | Not Applicable | None |
| 9.5.0 | Physically secure all media. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.5.1 | Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location’s security at least annually. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.6.0 | Maintain strict control over the internal or external distribution of any kind of media, including the following: | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.6.1 | Classify media so the sensitivity of the data can be determined. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.6.2 | Send the media by secured courier or other delivery method that can be accurately tracked. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.6.3 | Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.7.0 | Maintain strict control over the storage and accessibility of media. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 11 - Remote Desktop Plan |
| 9.7.1 | Properly maintain inventory logs of all media and conduct media inventories at least annually. | MHC PCI environment does not utilize any data within the current scope of the PCI network. All data is inputted directly via virtual terminal to the Curbstone gateway which is an approved PCI application. If MHC decides to utilize a remote desktop PC plan that was discussed in the PCI Workshop then this control will need to be readdressed. | Not Applicable | 10 - Tablet Plan |
| 9.8.0 | Destroy media when it is no longer needed for business or legal reasons as follows: | MHC needs to ensure that all media both electronic and physical are destroyed after use. This is part of the procedure just need to ensure all branches are following this procedure. | In Progress | 10 - Tablet Plan |
| 9.8.1 | Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. | MHC needs to ensure that all media both electronic and physical are destroyed after use. This is part of the procedure just need to ensure all branches are following this procedure. | In Progress | 10 - Tablet Plan |
| 9.8.2 | Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 9.9.0 | Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. | MHC does not currently have any procedures for detecting tampering on the Android tablets. A procedure needs to be created for the business units to follow so the Androids are not being physically tampered. | Absent | 08 - Policy and Procedure Development |
| 9.9.1 | Maintain an up-to-date list of devices. The list should include the following: · Make, model of device · Location of device (for example, the address of the site or facility where the device is located) · Device serial number or other method of unique identification. | MHC through the mobile device management software does keep an inventory of the Android tablets that are within their PCI environment | Implemented | 10 - Tablet Plan |
| 9.9.2 | Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). | MHC does not currently have any procedures for detecting tampering on the Android tablets. A procedure needs to be created for the business units to follow so the Androids are not being physically tampered. | Absent | 08 - Policy and Procedure Development |
| 9.9.3 | Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: · Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. · Do not install, replace, or return devices without verification. · Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). · Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | MHC does not currently have any procedures for detecting tampering on the Android tablets. A procedure needs to be created for the business units to follow so the Androids are not being physically tampered. | Absent | 08 - Policy and Procedure Development |
| 9.10.0 | Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| *Requirement 10: Track and monitor all access to network resources and cardholder data* | | | | |
| 10.1.0 | Implement audit trails to link all access to system components to each individual user. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.0 | Implement automated audit trails for all system components to reconstruct the following events: | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.1 | All individual user accesses to cardholder data | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | 10 - Tablet Plan |
| 10.2.2 | All actions taken by any individual with root or administrative privileges | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.3 | Access to all audit trails | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.4 | Invalid logical access attempts | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.5 | Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.6 | Initialization, stopping, or pausing of the audit logs | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.2.7 | Creation and deletion of system- level objects | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.0 | Record at least the following audit trail entries for all system components for each event: | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.1 | User identification | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.2 | Type of event | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.3 | Date and time | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.4 | Success or failure indication | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.5 | Origination of event | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.3.6 | Identity or name of affected data, system component, or resource. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.4.0 | Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.4.1 | Critical systems have the correct and consistent time. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.4.2 | Time data is protected. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.4.3 | Time settings are received from industry-accepted time sources. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.0 | Secure audit trails so they cannot be altered. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.1 | Limit viewing of audit trails to those with a job-related need. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.2 | Protect audit trail files from unauthorized modifications. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.4 | Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.5.5 | Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.6.0 | Review logs and security events for all system components to identify anomalies or suspicious activity. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.6.1 | Review the following at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.6.2 | Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.6.3 | Follow up exceptions and anomalies identified during the review process. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.7.0 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| 10.8.0 | Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: · Firewalls · IDS/IPS · FIM · Anti-virus · Physical access controls · Logical access controls · Audit logging mechanisms · Segmentation controls (if used) | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 10.8.1 | Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: · Restoring security functions · Identifying and documenting the duration (date and time start to end) of the security failure · Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause · Identifying and addressing any security issues that arose during the failure · Performing a risk assessment to determine whether further actions are required as a result of the security failure · Implementing controls to prevent cause of failure from reoccurring · Resuming monitoring of security controls | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 10.9.0 | Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | 03 - Logging and Monitoring |
| *Requirement 11: Regularly test security systems and processes.* | | | | |
| 11.1.0 | Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. | Though MHC does not have a rogue wireless monitoring program, they do have compensating controls at the network layer to render these devices invalid if they are added to the network. At the most the only thing the users utilizing a rogue access point would gain is access to the guest internet which itself has a registration process. | In Progress | 02 - Update Network Diagram and Configurations |
| 11.1.1 | Maintain an inventory of authorized wireless access points including a documented business justification. | MHC maintains an inventory of all approved/authorized wireless access points located in their enterprise. | Implemented | None |
| 11.1.2 | Implement incident response procedures in the event unauthorized wireless access points are detected | Though MHC does not have a rogue wireless monitoring program, they do have compensating controls at the network layer to render these devices invalid if they are added to the network. At the most the only thing the users utilizing a rogue access point would gain is access to the guest internet which itself has a registration process. | In Progress | 04 - Incident Response |
| 11.2.0 | Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 07 - Penetration Testing |
| 11.2.1 | Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 05 - Vulnerability Management |
| 11.2.2 | Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 05 - Vulnerability Management |
| 11.2.3 | Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified person | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 05 - Vulnerability Management |
| 11.3.0 | Implement a methodology for penetration testing that includes the following: · Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) · Includes coverage for the entire CDE perimeter and critical systems · Includes testing from both inside and outside the network · Includes testing to validate any segmentation and scope-reduction controls · Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 · Defines network-layer penetration tests to include components that support network functions as well as operating systems · Includes review and consideration of threats and vulnerabilities experienced in the last 12 months · Specifies retention of penetration testing results and remediation activities results. | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 05 - Vulnerability Management |
| 11.3.1 | Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 07 - Penetration Testing |
| 11.3.2 | Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 07 - Penetration Testing |
| 11.3.3 | Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 05 - Vulnerability Management |
| 11.3.4 | If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. | MHC does not perform any penetration testing, internal or external network vulnerabilities scanning. | Absent | 07 - Penetration Testing |
| 11.3.4.1 | Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 11.4.0 | Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | None |
| 11.5.0 | Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 11.5.1 | Implement a process to respond to any alerts generated by the change- detection solution. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 11.6.0 | Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| *Requirement 12: Maintain a policy that addresses information security for all personnel.* | | | | |
| 12.1.0 | Establish, publish, maintain, and disseminate a security policy. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 12.1.1 | Review the security policy at least annually and update the policy when the environment changes. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 12.2.0 | Implement a risk-assessment process that: · Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), · Identifies critical assets, threats, and vulnerabilities, and · Results in a formal, documented analysis of risk. | MHC does not have a risk assessment program for the IT department. | Absent | 06 - Risk Management |
| 12.3.0 | Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: | MHC does not have usage policies for the critical technologies within the MHC PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 08 - Policy and Procedure Development |
| 12.3.1 | Explicit approval by authorized parties | MHC does not have usage policies for the critical technologies within the MHC PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 08 - Policy and Procedure Development |
| 12.3.2 | Authentication for use of the technology | MHC does not have usage policies for the critical technologies within the MHC PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 08 - Policy and Procedure Development |
| 12.3.3 | A list of all such devices and personnel with access | MHC does not have usage policies for the critical technologies within the MHC PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 08 - Policy and Procedure Development |
| 12.3.4 | A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) | MHC is currently providing asset tags to their tablets and are determining the owners’ location, there will be some tablets in their environment that will be shared among multiple individuals. The tablets if compromised cannot get back to the MHC corporate or PCI environment. Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. | In Progress | 10 - Tablet Plan |
| 12.3.5 | Acceptable uses of the technology | MHC is currently providing asset tags to their tablets and are determining the owners’ location, there will be some tablets in their environment that will be shared among multiple individuals. The tablets if compromised cannot get back to the MHC corporate or PCI environment. Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. | In Progress | 10 - Tablet Plan |
| 12.3.6 | Acceptable network locations for the technologies | MHC is currently providing asset tags to their tablets and are determining the owners’ location, there will be some tablets in their environment that will be shared among multiple individuals. The tablets if compromised cannot get back to the MHC corporate or PCI environment. Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. | In Progress | 10 - Tablet Plan |
| 12.3.7 | List of company-approved products | MHC is currently providing asset tags to their tablets and are determining the owners’ location, there will be some tablets in their environment that will be shared among multiple individuals. The tablets if compromised cannot get back to the MHC corporate or PCI environment. Once the rollout of the branches has been completed this can change from In Progress to Implemented for the tablet plan. | In Progress | 10 - Tablet Plan |
| 12.3.8 | Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity | MHC is not utilizing remote-access technologies in the current PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | None |
| 12.3.9 | Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use | MHC is not utilizing remote-access technologies in the current PCI environment. If MHC changes to a PC based plan, then they will need to address this control requirement. | Not Applicable | None |
| 12.3.10 | For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | None |
| 12.4.0 | Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | MHC continues to establish their policy and procedure documentation. | In Progress | 08 - Policy and Procedure Development |
| 12.4.1 | Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: · Overall accountability for maintaining PCI DSS compliance · Defining a charter for a PCI DSS compliance program and communication to executive management | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 12.5.0 | Assign to an individual or team the following information security management responsibilities: | MHC continues to establish their policy and procedure documentation and will utilize their learning management system for awareness tracking in the environment. | In Progress | 08 - Policy and Procedure Development |
| 12.5.1 | Establish, document, and distribute security policies and procedures. | MHC continues to establish their policy and procedure documentation and will utilize their learning management system for awareness tracking in the environment. | In Progress | 08 - Policy and Procedure Development |
| 12.5.2 | Monitor and analyze security alerts and information, and distribute to appropriate personnel. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 12.5.3 | Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 12.5.4 | Administer user accounts, including additions, deletions, and modifications. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 12.5.5 | Monitor and control all access to data. | Currently, there are no systems within the MHC PCI environment that could house this requirement. If MHC changes to a PC based plan, then they will need to address this control requirement. | Absent | 03 - Logging and Monitoring |
| 12.6.0 | Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. | MHC continues to establish their policy and procedure documentation and will utilize their learning management system for awareness tracking in the environment. | In Progress | 08 - Policy and Procedure Development |
| 12.6.1 | Educate personnel upon hire and at least annually. | MHC continues to establish their policy and procedure documentation and will utilize their learning management system for awareness tracking in the environment. | In Progress | 08 - Policy and Procedure Development |
| 12.6.2 | Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | MHC continues to establish their policy and procedure documentation and will utilize their learning management system for awareness tracking in the environment. | In Progress | 08 - Policy and Procedure Development |
| 12.7.0 | Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) | MHC does follow human resource best practices for their hiring process. | Implemented | None |
| 12.8.0 | Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: | MHC is not storing any cardholder data on their system. All cardholder data is being inputted into approved PIN Transaction Security device and an approved terminal PCI approved virtual terminal that is provided by Curbstone. | Not Applicable | None |
| 12.8.1 | Maintain a list of service providers including a description of the service provided. | MHC needs to formalize the requirement to gather from Curbstone and the PAX terminal vendor the information in requirement 12.8.1-5. | In Progress | 09 - Vendor Management |
| 12.8.2 | Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | MHC needs to formalize the requirement to gather from Curbstone and the PAX terminal vendor the information in requirement 12.8.1-5. | In Progress | 09 - Vendor Management |
| 12.8.3 | Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | MHC needs to formalize the requirement to gather from Curbstone and the PAX terminal vendor the information in requirement 12.8.1-5. | In Progress | 09 - Vendor Management |
| 12.8.4 | Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. | MHC needs to formalize the requirement to gather from Curbstone and the PAX terminal vendor the information in requirement 12.8.1-5. | In Progress | 09 - Vendor Management |
| 12.8.5 | Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | MHC needs to formalize the requirement to gather from Curbstone and the PAX terminal vendor the information in requirement 12.8.1-5. | In Progress | 09 - Vendor Management |
| 12.9.0 | Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 12.10.0 | Implement an incident response plan. Be prepared to respond immediately to a system breach. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.1 | Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: · Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum · Specific incident response procedures · Business recovery and continuity procedures · Data backup processes · Analysis of legal requirements for reporting compromises · Coverage and responses of all critical system components · Reference or inclusion of incident response procedures from the payment brands. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.2 | Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.3 | Designate specific personnel to be available on a 24/7 basis to respond to alerts. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.4 | Provide appropriate training to staff with security breach response responsibilities. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.5 | Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.10.6 | Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | MHC has some structure in place for incident response, but are not formally structured and developed. MHC needs to fully implement an incident response program for their entire environment. | In Progress | 04 - Incident Response |
| 12.11.0 | Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: · Daily log reviews · Firewall rule-set reviews · Applying configuration standards to new systems · Responding to security alerts · Change management processes | Not applicable to MHC as they are not a service provider | Not Applicable | None |
| 12.11.1 | Additional requirement for service providers only: Maintain documentation of quarterly review process to include: · Documenting results of the reviews · Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program | Not applicable to MHC as they are not a service provider | Not Applicable | None |