YourIT!
Your Logo Goes Here

PCI Assessment

PCI Policy and Procedures

Prepared for:
YourIT Client
Prepared by:
MyIT Company

Table of Contents

1

2 Overall Risk

2.1 Conduct Risk Analysis

Policy: A comprehensive Risk Analysis of all our assets including Information Systems will be conducted periodically and involves identifying risk and vulnerabilities in our information systems. To do this we will conduct an accurate and thorough assessment of the potential threats and vulnerabilities to the confidentiality, integrity and availability of cardholder data at our office. Then we will reduce the risks and vulnerabilities to an appropriate and reasonable level or to the greatest extent possible though ongoing management. The risk analysis will be performed following industry best practice standards. A Risk Analysis will be completed no less than one time a year or after successful implementation of any major system change. Major system change would include an office relocation, replacement of system component containing cardholder data, etc. In addition, an abbreviated form of the Risk Assessment called a Risk Profile will be performed monthly to identify and prioritize risks to cardholder data.

Procedure: The objective of the Risk Assessment is to complete comprehensive, periodic and independent review of our security vulnerabilities. We will start a risk assessment with a current inventory of all know devices and applications on our network and we will "map" or diagram their interdependencies so we can better understand the complex relationships between applications and devices. We will also identify frequency and format of the risk assessment (self-risk assessment versus third-party, independent risk assessment), and document it. The risk assessment process will include review of administrative, physical and technical safeguards, and also take into consideration criticality, impact and creation of recommendations identifying mitigation strategies. The Risk Assessment will include a risk score for measurement and ongoing change analysis and an executive level summary report in narrative form. An automated Risk Profile will be performed monthly. A more comprehensive Risk Analysis involving more manual input through on-site surveys as well as using automated data collection routines will be performed, at least, annually or in the event of a significant change (office move, changing the cardholder data environment system, moving servers to the cloud, etc.) or conducted at the direction of the Cardholder Data Security Officer.

2.2 Risk Management

Policy: Once we have completed the risk analysis process, the next step is risk management. Risk management, required by PCI DSS Requirements, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of cardholder data and protect against any reasonably anticipated threats, hazards, or disclosures of cardholder data not permitted by the Card Issuers and/or Acquiring Banks, or the Cardholder themselves.
The first step in the risk management process should be to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls. The risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their risk score.
An important component of the Risk Management Plan is the plan for implementation of the selected security measures and controls. The implementation component of the plan should address:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation of measures and controls selected to reduce the risk of an issue;
- Implementation project priorities, such as required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstance. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors we must consider when determining measures and controls to fix an issue. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate. The output of this step is a Risk Management Plan that contains prioritized risks, options for mitigation of those risks, and a plan for implementation. The plan will guide our actual implementation of security measures to reduce risks to cardholder data to reasonable and appropriate levels.
The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.
Procedure: The objective of risk management is to create and document a planned risk management approach as follows:

A. The most recent Risk Assessment shall be used to develop or modify the risk Management Plan.
B. The Management Plan shall include implementation specifics and prioritized timelines for selected risk mitigation strategies identified in the monthly Risk Profiles, or Risk Assessment report.
C. The Security Officer or designated third party will execute the Management Plan by reviewing and addressing issues identified therein and will be responsible for implementation of the IT security, network and system recommendations.

We will implement automated tools and use other means to continually review and evaluate systems and devices that might store or have access to cardholder data. We will conduct a regular inventory of our information systems containing cardholder data and the security measures used to protect those systems. We will give highest priority to fixing issues associated with unacceptably high risk rankings and will then work to minimize or eliminate the risk based upon feasibility and effectiveness of specific method. Our Cardholder Data Security Officer will oversee the implementation of solutions to better secure systems that store, process or transmit electronic cardholder data

Automated tools will be used to validate that remediation has occurred and reports will be archived for at least TBD years. The tool activities will focus on collecting data through open protocols across the network or operating systems and producing reports and analysis on antivirus, patch and reliability, for example. We will complement the automated reporting with walk through audits, device inspections and user list reviews.

3 Overview

This document enumerates the policies and procedures pursuant to PCI DSS Version 3 and adopted by us to comply with technological aspects of the PCI DSS Requirements as required under our agreement with our Payment Brand Card issuer's Acquiring Bank. The policies are intended to ensure the confidentiality, integrity and availability of cardholder data residing on our networks and computers and the transmission of data outside of our networks when appropriate. These policies and procedures do not cover every condition, clause or stipulation of the PCI DSS Requirements nor were they intended to. The processes adopted by our organization herein are designed to automate the documentation and reporting of technological requirements and not, for example, tasks that involve administrative attention such as employee background checks, sanction warnings or breach notification. The following policies and procedures support the Administrative, Physical, and Technical safeguards of the Cardholder Data Environment, its system components, and/or cardholder data whether required or addressable, to the extent described below as follows:

High Level PCI DSS Requirement Category	PCI DSS Requirement	Requirement Description
Build and Maintain a Secure Network	1	Install and maintain firewall to protect cardholder data
Build and Maintain a Secure Network	2	Prohibition of vendor-supplied default password for systems and security parameters
Build and Maintain a Secure Network	2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts
Build and Maintain a Secure Network	2.2	Develop configuration standards for all system components
Build and Maintain a Secure Network	2.2.1	Implement only one primary function per server
Build and Maintain a Secure Network	2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system
Build and Maintain a Secure Network	2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure
Build and Maintain a Secure Network	2.2.4	Configure system security parameters to prevent misuse
Build and Maintain a Secure Network	2.2.5	Remove all unnecessary functionality
Build and Maintain a Secure Network	2.3	Encrypt all non-console administrative access using strong cryptography
Protect Cardholder Data	3	Protection of stored data
Protect Cardholder Data	3.1	(not covered)
Protect Cardholder Data	3.2	Do not store sensitive authentication data after authorization
Protect Cardholder Data	3.2.1	(not covered)
Protect Cardholder Data	3.2.2	Do not store the card verification code use to verify card-not-present transactions
Protect Cardholder Data	3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block
Protect Cardholder Data	4	Encrypt transmission of cardholder data across open, public networks

Protect Cardholder Data	4.1	Use strong cryptography and security protocols to safeguard cardholder data during transmission
Protect Cardholder Data	4.2	Never send unprotected Personal Account Numbers (PANs) by end-user messaging technologies
Maintain a Vulnerability Management Program	5	Protection Against Malicious Software
Maintain a Vulnerability Management Program	5.1	Deploy anti-virus software on all systems affected by malicious software
Maintain a Vulnerability Management Program	5.1.1	Ensure that anti-virus programs can detect, remove and protect against all types of malicious software
Maintain a Vulnerability Management Program	5.1.2	Review systems not commonly affected by malicious software to confirm that systems do not require anti-virus software
Maintain a Vulnerability Management Program	5.2	Ensure that all anti-virus mechanisms are kept current, perform scans and generate logs as required
Maintain a Vulnerability Management Program	5.3	Ensure that anti-virus mechanisms are running and cannot be disabled unless authorized
Maintain a Vulnerability Management Program	6	Develop and maintain secure systems and applications
Maintain a Vulnerability Management Program	6.1	Establish process to identify security vulnerabilities using reputable outside sources
Maintain a Vulnerability Management Program	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches
Maintain a Vulnerability Management Program	6.3	(not covered)
Maintain a Vulnerability Management Program	6.4	Follow change control processes and procedures
Maintain a Vulnerability Management Program	6.4.1	(not covered)
Maintain a Vulnerability Management Program	6.4.2	(not covered)
Maintain a Vulnerability Management Program	6.4.3	(not covered)
Maintain a Vulnerability Management Program	6.4.4	(not covered)
Maintain a Vulnerability Management Program	6.4.5	Change control procedures for the implementation of security patches and software modifications
Maintain a Vulnerability Management Program	6.4.5.1	Documentation of impact
Maintain a Vulnerability Management Program	6.4.5.2	Documented approval by authorized parties
Maintain a Vulnerability Management Program	6.4.5.3	Functionality testing
Maintain a Vulnerability Management Program	6.4.5.4	Back-out procedures
Maintain a Vulnerability Management Program	6.5	Address common code vulnerabilities

Maintain a Vulnerability Management Program	6.5.1	Injection flaws
Maintain a Vulnerability Management Program	6.5.2	Buffer overflow
Maintain a Vulnerability Management Program	6.5.3	(not covered)
Maintain a Vulnerability Management Program	6.5.4	(not covered)
Maintain a Vulnerability Management Program	6.5.5	(not covered)
Maintain a Vulnerability Management Program	6.5.6	(not covered)
Maintain a Vulnerability Management Program	6.5.7	Cross-site scripting (XSS)
Maintain a Vulnerability Management Program	6.5.8	Improper access control
Maintain a Vulnerability Management Program	6.5.9	Cross-site request forgery
Maintain a Vulnerability Management Program	6.5.10	Broken authentication and session management
Implement Strong Access Control Measures	7	Restricted access to cardholder data
Implement Strong Access Control Measures	7.1	Limit access to system components and cardholder data
Implement Strong Access Control Measures	7.1.1	(not covered)
Implement Strong Access Control Measures	7.1.2	Limit access to system components and cardholder data
Implement Strong Access Control Measures	7.1.3	Assign access based on individual personnel's job classification and function
Implement Strong Access Control Measures	8	Access to Cardholder Data Environment (CDE) system components
Implement Strong Access Control Measures	8.1	Proper User Identification Management for Non-Consumer Users and Administrators
Implement Strong Access Control Measures	8.1.1	Unique User Identification
Implement Strong Access Control Measures	8.1.2	(not covered)
Implement Strong Access Control Measures	8.1.3	Termination Procedures
Implement Strong Access Control Measures	8.1.4	(not covered)
Implement Strong Access Control Measures	8.1.5	Third-Party User ID Management, System Component Access, and Monitoring
Implement Strong Access Control Measures	8.1.6	Repeated login access attempts
Implement Strong Access Control Measures	8.1.7	User ID lockout duration

Implement Strong Access Control Measures	8.2	Ensuring proper user-authentication management
Implement Strong Access Control Measures	8.2.1	Encryption of all authentication credentials
Implement Strong Access Control Measures	8.2.2	(not covered)
Implement Strong Access Control Measures	8.2.3	Password strength and complexity
Implement Strong Access Control Measures	8.2.4	Password expiration policy
Implement Strong Access Control Measures	8.2.5	New password/phrase requirements
Implement Strong Access Control Measures	8.2.6	Password/phrase first-time use and reset requirements
Implement Strong Access Control Measures	8.3.2	Multi-Factor authentication requirement for remote network access by users
Implement Strong Access Control Measures	8.4	(not covered)
Implement Strong Access Control Measures	8.5	Group, shared, and Generic IDs prohibition policy
Implement Strong Access Control Measures	8.6	Authentication mechanism use assignments
Implement Strong Access Control Measures	9	Controlling physical access to cardholder data
Implement Strong Access Control Measures	9.1	Facility entry controls and monitoring physical access to systems in the cardholder data environment
Implement Strong Access Control Measures	9.2	(not covered)
Implement Strong Access Control Measures	9.3	(not covered)
Implement Strong Access Control Measures	9.4	(not covered)
Implement Strong Access Control Measures	9.5	Physically securing all media
Implement Strong Access Control Measures	9.6	Controls over internal and external distribution of any kind of media
Implement Strong Access Control Measures	9.6.1	Media classification to determine sensitivity
Implement Strong Access Control Measures	9.6.2	Send media by secured courier or other delivery method that can be tracked
Implement Strong Access Control Measures	9.6.3	Management notification and approval of all media moved from a secured area
Implement Strong Access Control Measures	9.7	Maintain strict control over media storage and accessibility
Implement Strong Access Control Measures	9.8	Media destruction policy
Regularly Monitor and Test Networks	10	Track and monitor access to network resources and cardholder data

Regularly Monitor and Test Networks	10.1	(not covered)
Regularly Monitor and Test Networks	10.2	Automated audit trails for all system components
Regularly Monitor and Test Networks	10.2.1	(not covered)
Regularly Monitor and Test Networks	10.2.2	Generate audit trail of all actions taken by any individual with root or administrative privileges
Regularly Monitor and Test Networks	10.2.3	(not covered)
Regularly Monitor and Test Networks	10.2.4	Generate audit trails of invalid logical access attempts
Regularly Monitor and Test Networks	10.2.5	Generate audit trails of the use of and changes to identification and authentication mechanisms
Regularly Monitor and Test Networks	10.3	Recording audit trail entries for all system components for each event
Regularly Monitor and Test Networks	10.4	(not covered)
Regularly Monitor and Test Networks	10.5	Securing audit trails to prevent alteration
Regularly Monitor and Test Networks	10.5.1	(not covered)
Regularly Monitor and Test Networks	10.5.2	(not covered)
Regularly Monitor and Test Networks	10.5.3	(not covered)
Regularly Monitor and Test Networks	10.5.4	Write logs for external-facing technologies on a secure log server or media device
Regularly Monitor and Test Networks	10.6	Review logs and security events for all system components
Regularly Monitor and Test Networks	10.6.1	Daily review of security events including logs of system components, critical system components, and servers that perform security functions
Regularly Monitor and Test Networks	10.6.2	Review logs of all other system components periodically based on risk management strategy and annual risk assessment
Regularly Monitor and Test Networks	10.6.3	Follow up exceptions and anomalies identified during the review process
Regularly Monitor and Test Networks	10.7	Retain audit trail history
Regularly Monitor and Test Networks	11	Regular testing of security systems and processes
Regularly Monitor and Test Networks	11.1	(not covered)
Regularly Monitor and Test Networks	11.2	(not covered)
Regularly Monitor and Test Networks	11.2.1	(not covered)
Regularly Monitor and Test Networks	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)

Regularly Monitor and Test Networks	11.2.3	Perform internal and external scans, and rescans as needed, after any significant change
Regularly Monitor and Test Networks	11.3	Penetration testing
Regularly Monitor and Test Networks	11.3.1	Network-layer penetration tests
Regularly Monitor and Test Networks	11.3.2	(not covered)
Regularly Monitor and Test Networks	11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections
Regularly Monitor and Test Networks	11.3.4	Segmentation
Regularly Monitor and Test Networks	11.4	(not covered)
Regularly Monitor and Test Networks	11.5	Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files
Regularly Monitor and Test Networks	11.5.1	Implement a process to respond to any alerts generated by the change-detection solution
Maintain an Information Security Policy	12	Information security policy for all personnel
Maintain an Information Security Policy	12.1	Establish, publish, maintain, and disseminate a security policy
Maintain an Information Security Policy	12.2	(not covered)
Maintain an Information Security Policy	12.3	(not covered)
Maintain an Information Security Policy	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel
Maintain an Information Security Policy	12.5	Assign to an individual or team the following information security management responsibilities
Maintain an Information Security Policy	12.5.1	(not covered)
Maintain an Information Security Policy	12.5.2	(not covered)
Maintain an Information Security Policy	12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
Maintain an Information Security Policy	12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security
Maintain an Information Security Policy	12.7	(not covered)
Maintain an Information Security Policy	12.8	Maintain and implement policies and procedures to manager service providers with whom cardholder data is shared, or that could affect the security of cardholder data
Maintain an Information Security Policy	12.8.1	Maintain a list of service providers
Maintain an Information Security Policy	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
Maintain an Information Security Policy	12.8.3	Ensure there is an established process for engaging service providers, including proper due diligence prior to engagement
Maintain an Information Security Policy	12.8.4	Maintain a program to monitor service providers PCI DSS compliance status at least annually
Maintain an Information Security Policy	12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity
Maintain an Information Security Policy	12.9	(not covered)
Maintain an Information Security Policy	12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach
Maintain an Information Security Policy	12.10.1	Create the incident response plan to be implemented in the event of a breach

4 Build and Maintain a Secure Network

4.1 Install and maintain firewall to protect cardholder data

PCI DSS Requirement 1.0 – Install and maintain a firewall configuration to protect cardholder data

Policy: We will protect our network perimeter with a business-class firewall to prevent unauthorized access to Cardholder Data. The firewall must incorporate Intrusion Prevention and Intrusion Detection services and reporting to validate that the protection is enabled and working.
Firewall implementations must adhere to the following guidelines consistent with the PCI DSS Requirements and Standards:

- 1.1.4 - Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

- 1.1.6 - Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

- 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data
    - 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

    - 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.
- 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

    - 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)

    - 1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

    - 1.3.5 Permit only “established” connections into the network.

    - 1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to:
        - Network Address Translation (NAT),
        - Placing servers containing cardholder data behind proxy servers/firewalls,
        - Removal or filtering of route advertisements for private networks that employ

registered addressing

- Internal use of RFC1918 address space instead of registered addresses.

- 1.4 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.

Procedure: We will use automated software data collection and report analysis to identify the manufacturer and model of the network firewall, and determine what security features are installed and enabled. Security subscriptions will be evaluated to ensure they are current.

4.2 Prohibition of vendor-supplied default password for systems and security parameters

PCI DSS Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters

Policy: We recognize that the use of vendor default passwords and other default settings within system components and applications can provide malicious individuals (internal and external) with the ability to compromise systems. Vendor-supplied details, system passwords and other security parameters are disabled or removed from system components prior to installation within the network.

Procedure: We will use automated software data collection and report analysis to identify and review all system components' configurations to ensure their configuration adheres to the guidelines above.

4.2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts

PCI DSS Requirement 2.1 - 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.).

Policy: In an effort to prevent malicious individuals from using vendor default settings, account names and passwords to compromise operating system software, payment applications, software that provides security services, and the systems that they are installed, it is our policy that all vendor default settings account names and passwords are removed or disabled from any system component before it is installed on the network. This applies to ALL DEFAULT PASSWORDS.

Procedure:

- Before any system component is connected to the network, the password for the component's vendor-supplied default user account is to be changed.

- Then all unnecessary vendor-supplied default accounts are to either be disabled or removed.

ALL DEFAULT PASSWORDS/Accounts include, but not limited to, those used by operating systems, software that provides security services, payment applications and system accounts , POS terminals, Simple Network Management Protocol (SNMP) community strings, etc. that will operate on or with one or more system components.

- We will use automated software data collection and report analysis to identify and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines above.

4.2.2 Develop configuration standards for all system components

PCI DSS Requirement 2.2 - 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)

Policy: We recognize the need and value to develop configuration standards for all system components and to assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Our system component configuration standards have been developed to address all known security vulnerabilities and rely upon one or more industry accepted hardening standards

Procedure: Document all system component hardening standards and train personnel on the system component configuration, installation, and implementation of components to ensure that all known security vulnerabilities have been addressed and in compliance with this policy.

On a regular basis, these configuration standards will be amended and updated to take into consideration new or improved versions of system components, newly identified vulnerabilities, and the ongoing development of the security hardening standards themselves.

Training Consideration: System administrators and cardholder data environment IT system service personnel should be trained to implement defined system component configuration hardening standards.

4.2.2.1 Implement only one primary function per server

PCI DSS Requirements 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.)

Policy: When implementing system components and servers within the cardholder data environment, we assess the security needs that must be met by server operating applications, databases and other software that require its own security level and to prevent functions with two different security levels from co-existing on the same server. It is our policy and practice to only implement one primary function per server will be implemented. Functions may include, for example, web servers, database servers, application servers, DNS, and others. During server deployment we will identify the security needs of the system and the security levels of a specific function and implement only one primary function per server to prevent different security levels from co-existing on the same server.

Procedure: We will use automated software data collection and report analysis to identify and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines above.

4.2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system

PCI DSS Requirements 2.2.2 - Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

Policy: We recognize that there are many protocols that may be implemented with desire or default that are commonly used by malicious individuals to compromise a network. Therefore, our configuration standards and system component implementation processes are defined to ensure that only necessary services and protocols are enabled. During system component configuration and deployment on the necessary protocols, daemons, etc. as required will be enabled to support the function of the system.

Procedure: We will use automated software data collection and report analysis to identify and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines above.

4.2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure

PCI DSS Requirement 2.2.3 - Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

Policy: For any required services, protocols, or daemons that are considered to be insecure that are used in conjunction with the system components and applications implemented within the cardholder data environment, our configuration standards require that we implement additional security secured technologies such as SSH, S-FTP, SSL, and/or IPSec VPN to protect insecure services that may include, but are not limited to, NetBIOS, file-sharing, Telnet, FTP, etc.

Procedure: We will use automated software data collection and report analysis to identify and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines above.

4.2.2.4 Configure system security parameters to prevent misuse

PCI DSS Requirement 2.2.4 - Configure system security parameters to prevent misuse.

Policy: Our configuration standards and system component implementation processes are defined to specifically address security settings and parameters that have known security implements for each type of system when in use. Personnel responsible for configuration and/or administering systems are to be trained and knowledgeable in the specific security parameters and settings that are to be applied during system component implementation.

Procedure: Use automated software and reporting to validate that system component configurations are implemented with security settings and parameters that prevent misuse of the system components and other functions.

Training Considerations: Personnel responsible for configuration and/or administering system components and functions are to be knowledgeable and trained in the specifics of the settings and security parameters used when configuring system components and functions.

4.2.2.5 Remove all unnecessary functionality

PCI DSS Requirement 2.2.5 - Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Policy: We will remove unnecessary functions from system components and servers during configuration and prior to deployment within the cardholder data environment. Unnecessary functionality includes, but is not limited to, scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Procedure: Use automated software and reporting to validate that system component and server configurations are implemented with unnecessary functionality.

4.2.3 Encrypt all non-console administrative access using strong cryptography

PCI DSS Requirement 2.3 - Encrypt all non-console administrative access using strong cryptography.

Note: *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*

Policy: All non-console administrative access to system components in the cardholder data environment will be encrypted using strong cryptography. We utilize encryption technologies such as SSH, VPN, or SSL/TLS to encrypt all web-based management and other non-console administrative access to system components.

Procedure: Use automated software and reporting to validate that all web-based management and non-console administrative access is configured to use strong cryptography.

5 Protect Cardholder Data

5.1 Protection of stored cardholder data

PCI DSS Requirement 3 - Protect stored cardholder data

Policy: We employ risk mitigation practices whereby any stored cardholder data is protected through the use of protection methods that may include encryption, truncation, masking and hashing.

Additional protections implemented include processes and user training to ensure that unprotected cardholder data is not sent using end-user technologies such as e-mail and instant messaging.

Procedure: Use automated software and reporting to validate that all configurations of system components ensure that stored cardholder data is protected.

Training consideration: Train users to ensure that unprotected cardholder data is not sent using e-mail, instant messaging, or any other end-user messaging technology.

5.2 Do not store sensitive authentication data after authorization

PCI DSS Requirement 3.2 - 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.

It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:

* There is a business justification, and
* The data is stored securely.

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:

Policy: We do not store any cardholder transactions sensitive authentication data within the cardholder data environment system components and applications. System component configurations and applications are configured in accordance with entity configuration standards to prevent storage of sensitive authentication data in:

- incoming transaction data
- all logs
- history files
- trace files
- database schema
- database contents

Any sensitive data received is not stored after authorization and this data is deleted and rendered unrecoverable.

Procedure: Procedure: Use automated software and reporting to validate that all configurations of system components, applications and databases ensure that cardholder sensitive authentication data is not stored.

5.2.1.1 Do not store the card verification code use to verify card-not-present transactions

PCI DSS Requirement 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.

Policy: We do not store cardholder card verification codes or values should not be stored after card-not-present transaction authorizations.

Procedure: Use automated software and reporting to validate that all configurations of system components ensure that cardholder card verification codes or values are not stored after authorization.

System component data to be reviewed may include, but is not limited to:

- incoming transaction data
- all logs (for example, transaction, history, debugging, error)
- history files
- trace files
- several database schemas
- database contents

Training consideration: Train users/personnel perform job duties within the cardholder data environment that handle/process cardholder verification codes to not store verification codes after card transaction authorization.

5.2.1.2 Do not store the personal identification number (PIN) or the encrypted PIN block

PCI DSS Requirement 3.2.3 - Do not store the personal identification number (PIN) or the encrypted PIN block.

Policy: Cardholder personal identification number (PIN) or the encrypted PIN block should not be stored after card-not-present transaction authorizations.

Procedure: Use automated software and reporting to validate that all configurations of system components ensure that cardholder personal identification number (PIN) or the encrypted PIN block are not stored after authorization.

System component data to be reviewed may include, but is not limited to:

- incoming transaction data
- all logs (for example, transaction, history, debugging, error)
- history files
- trace files
- several database schemas
- database contents

Training consideration: Train users/personnel perform job duties within the cardholder data environment that handle/process cardholder PIN data to not store a cardholder PIN or the encrypted PIN block after authorization.

5.3 Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirement 4 - Encrypt transmission of cardholder data across open, public networks

Policy: All cardholder data transmitted across open, public networks is encrypted during transmission.

Procedure: Use automated software and reporting to validate that all configurations of system components are correctly configured to ensure that cardholder card is encrypted during transmission across open, public networks in compliance with the policy above.

5.3.1 Use strong cryptography and security protocols to safeguard cardholder data during transmission

PCI DSS Requirement 4.1 - 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. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*

Policy: We use strong cryptography and security protocols, including but not limited to, SSL/TLS, IPSEC, SSH, and others to protect sensitive cardholder data during transmission over open, public networks. Our configuration standards require that the strong cryptography implementation be used and that security protocols configurations will include the following:

- only trusted keys and certificates are accepted
- certificates are obtained from a recognized public certificate authority
- the protocol in use only supports secure versions or configurations
- the encryption strength is appropriate for the encryption methodology in use
- for SSL/TLS implementations that SSL/TLS is enabled whenever cardholder data is transmitted or received - (including browser based implementations where HTTPS appears as the browser URL protocol)

Procedure: We will use automated software data collection and report analysis to identify and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines to safeguard cardholder data during transmission.

5.3.2 Never send unprotected Personal Account Numbers (PANs) by end-user messaging technologies

PCI DSS Requirement 4.2 - Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

Policy: We recognize that sending any data via end-user messaging technologies that do not use strong encryption to protect data represents is a security risk. The sending of unprotected Personal Account Numbers (PANs) via end-user messaging technologies that are non-strong encrypted is prohibited.

In cases where PANs are to be sent via end-user messaging applications such as E-mail, instant messaging, and chat applications, these applications will be configured with strong encryption to protect PANs during transmission and storage.

Procedure: Maintain awareness among users within the cardholder data environment on the prohibition of sending unprotected PAN data via non-encrypted end-user messaging technologies.

For users that have an authorized business requirement to transmit PANs via end-user messaging technologies, these users will be provided with end-user messaging technologies that employ strong encryption for use in transmitting PANs as authorized.

Training consideration: Train users on the policy detailed above. Train users that are authorized to send "protected" PANs via end-user technologies that employ strong encryption on how to use these authorized for use end-user messaging systems.

6 Maintain a Vulnerability Management Program

6.1 Protection against Malicious Software

PCI DSS Requirement 5 - Protect all systems against malware and regularly update anti-virus software or programs

Policy: We will use industry best practices and anti-virus software or programs to protect all systems against malware and regularly update anti-virus software or programs.

Procedure: Anti-virus software will be deployed, kept up to date, run regularly, and monitored on all systems commonly affected by malicious software. Users in the cardholder data environment will also be trained on how to identify and report suspicious activity created as a result of malicious software.

6.1.1 Deploy anti-virus software on all systems affected by malicious software

PCI DSS Requirement 5.1 - Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

Policy: We will deploy anti-virus software and malicious software checking programs at the perimeter (edge) of the network and on individual end-user systems. We will subscribe to receiving and deploying updates to anti-virus and malicious software checking programs. We will conduct security training that will include information on:

- potential harm that can be caused by malicious software
- prevention of malicious software such as viruses
- steps to take if malicious software such as a virus is detected

Procedure: Utilize automated software and reporting to validate that anti-malware protection is installed and receives current definition updates on all applicable devices, including firewalls, servers, personal computers, and endpoint devices.

Training Considerations: End users should be trained to be wary of phishing e-mails and never click on links unless they are absolutely sure it is legitimate. They should also be taught not to connect thumb drives and other portable drives unless they are sure they come from a safe source.

6.1.1.1 Ensure that anti-virus programs can detect, remove and protect against all types of malicious software

PCI DSS Requirement 5.1.1 - Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

Policy: Anti-virus software or programs selected for use and deployment within the cardholder data environment and its applicable system components will be capable of detecting, removing, and protecting against all known types of malicious software. Malicious software to be detected may include viruses, trojans, worms, spyware, adware, rootkits, and their derivatives.

Procedure: Utilize automated software and reporting to validate that anti-malware protection is capable of detecting, removing and protecting against known types of malicious software on all applicable devices, including firewalls, servers, personal computers, and endpoint devices.

6.1.1.2 Review systems not commonly affected by malicious software to confirm that systems do not require anti-virus software

PCI DSS Requirement 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.

Policy: We will perform periodic evaluations of systems within the cardholder data environment/network that are considered to be not commonly affected by malicious software. This periodic evaluation will be used to determine if these systems can continue to operate without anti-virus software or programs installed and operational. These systems may include mainframes, mid-range computers and similar systems that are within the cardholder data environment.

Procedure: Perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such and not require anti-virus software. If threats are identified, then industry best practices and risk management measures must be taken and documented. Such measures may include, but are not limited to, installing anti-virus software or programs.

6.1.2 Ensure that all anti-virus mechanisms are kept current, perform scans and generate logs as required

PCI DSS Requirement 5.2 - 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.

Policy: We have defined and implemented industry best practices and reporting procedures to ensure that anti-virus mechanisms implemented within the cardholder data environment are maintained as follows:

- Are kept current
- Perform periodic scans
- Generate audit logs where the logs are retained per PCI DSS Requirement 10.7, in particular, logs are retained for a period one (1) year, and there are at least the last three (3) months' logs immediately available for analysis

6.1.3 Ensure that anti-virus mechanisms are running and cannot be disabled unless authorized

PCI DSS Requirement 5.3 - 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.

Policy: Our established anti-virus configuration and implementation guidelines and practices require that anti-virus mechanisms are actively running at all times and are configured to prevent the mechanisms from being disabled or altered by users.

In the case that anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Upon approval, sdditional security measures may be implemented or exercised for the period of time during which anti-virus protection is not active

Procedure: We will use automated software data collection and report analysis to identify and review all anti-virus mechanisms on systems and ensure that these mechanisms are configured to operate in a fashion that adheres to the guidelines above.

Note: In cases where official authorization and approval has been given to disable anti-virus protection on a system component, additional security measures will be implemented while the anti-virus mechanism is not active. Such measures may include , disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after the anti-virus mechanism it is re-enabled.

6.2 Develop and maintain secure systems and applications

PCI DSS Requirement 6 - Develop and maintain secure systems and applications

Policy: We recognize that it is important to develop and maintain secure systems and applications to prevent malicious individuals from gaining privileged access to system components and applications.

Our policy to develop and maintain secure systems and application ensures that:

- all systems must have all appropriate software patches to protect against exploitation and compromise of cardholder data
- the entities responsible for managing system components and applications are to install vendor-provided security patches as they become available
- vulnerabilities for in-house developed applications are avoided through the use of best practices and standard coding techniques

Procedure:

- we will use automated software data collection and report analysis to identify and review all system components and applications to ensure that the appropriate vendor-provided patches are installed to protect the cardholder data environment
- entities that manage system components and applications will install vendor-supplied security patches.
- prior to installing vendor-provided patches an impact assessment will be performed by evaluating and testing the patches to ensure their installation does not conflict with existing security configurations.
- security vulnerabilities associated with application development techniques will be avoided through the:
    - use of standard system development processes
    - employment of secure coding techniques

6.2.1 Establish process to identify security vulnerabilities using reputable outside sources

PCI DSS Requirement 6.1 - 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.

Policy: We have a process to identify security vulnerabilities through:

- using methods for evaluating vulnerabilities and assigning risk ratings that vary based on our organization's environment and risk assessment strategy
- using reputable outside sources
- assigning a risk ranking of vulnerabilties as "high", "medium", or "low" to newly discovered security vulnerabilities
- requiring that risk rankings are to be based on industry best practices as well as consideration of potential impact on the cardholder data environment
- using criteria for ranking vulnerabilities that will include, but are not limited to:
    - CVSS based scoring
    - classification of the vulnerability by the system component/application third party
    - the type of system components and/or applications affected
- A risk rating of "critical" may be assigned to critical system components and applications that may include, but are not limited to:
    - security systems
    - public-facing devices and systems
    - databases
    - and other systems that store, process, or transmit cardholder data

Procedure: We will use automated software data collection and report analysis to identify and review all system components and applications to ensure that the appropriate vendor-provided patches are installed to protect the cardholder data environment. We will use automated software data collection and report analysis to identify and review all vendor-provided services that are part of our cardholder data environment to ensure that services provided and their configurations adhere to the guidelines above.

6.2.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches

PCI DSS Requirements 6.2 - 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.

Policy: We ensure that all system components and software within the cardholder data environment are protected from known vulnerabilities installing by applicable vendor-supplied security patches.
Procedure:

- We use automated software data collection and report analysis to identify and review all system components and applications to ensure that the appropriate vendor-provided patches are installed to protect the cardholder data environment.

- Prior to installing vendor-supplied patches we will test and evaluate the patches to ensure that their implementation will not conflict with existing security configurations.
- Prioritize patch installation to ensure that critical or at-risk systems have patches installed within 1 month.
- Critical security patches will be installed within one month of release.
- Lower risk patches will be installed in an appropriate time (within 2-3 months).

6.2.3 Follow change control processes and procedures

PCI DSS Requirement 6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:

- In accordance with PCI DSS Self Assessment Questionnaire (SAQ) A-EP, the change control processes and procedures per PCI DSS Requirement 6.4.5

Policy: We use industry best practices, change control processes, and procedures to control, document, and authorize changes to the system components.

Procedure: Follow the cardholder data environment change control procedures as outlined in section PCI DSS Requirement 6.4.5 below.

6.2.3.1 Change control procedures for the implementation of security patches and software modifications

PCI DSS Requirement 6.4.5 - Change control procedures for the implementation of security patches and software modifications must include the following:

- Documentation of impact.
- Documented change approval by authorized parties.
- Functionality testing to verify that the change does not adversely impact the security of the system.
- Back-out procedures.

Policy: Per our documented security patch and software coding policies and procedures, all security patch(es) installations and software coding changes comply with industry best practices and standards for information system change control. Change control documentation must include the following:

- Documentation of impact of the security patch and/or software code changes.
- Documented change approval by authorized parties.
- Functionality testing to verify that installation of security patches, and/or implementation of software code changes do not adversely impact the security of the system.
- Security patch and software code change back-out procedures.

Procedure:

- **Documentation of impact:** an impact assessment must be performed and documented for all changes to the cardholder data environment resulting from the installation of security patches and software coding modifications.

- **Authorization and signoff:** prior to the implementation of any security patches and/or software coding modifications, a documented change control approval by authorized parties must be obtained.
- **Security Patches - Change functionality testing:** operational testing of the affected components and/or applications within the cardholder data environment must be tested to ensure that security patches do not adversely impact the security of the system.

We will use automated software data collection and report analysis to identify and review all system components and applications to ensure that the newly installed vendor-provided security patches have been installed to protect the cardholder data environment in compliance with the policy detailed above.

- **Software Modification - Change functionality testing:** operational testing of the affected components and/or applications within the cardholder data environment must be tested to ensure that software modifications do not adversely impact the security of the system.

For custom software code changes, testing of the changes to software applications must include compliance with PCI DSS Requirement 6.5.

- **Back-out procedures:** all back-out procedures are to be defined and documented prior to the implementation of security patches and software application modifications.

6.2.3.1.1 Documentation of impact

PCI DSS Requirement 6.4.5.1 – Documentation of impact

Refer to PCI DSS Requirement 6.4.5 policies and procedures referenced above.

6.2.3.1.2 Documented approval by authorized parties

PCI DSS Requirement 6.4.5.2 - Documented change approval by authorized parties

Refer to PCI DSS Requirement 6.4.5 policies and procedures referenced above.

6.2.3.1.3 Functionality testing

PCI DSS Requirement 6.4.5.3 - Functionality testing to verify that the change does not adversely impact the security of the system.

Refer to PCI DSS Requirement 6.4.5 policies and procedures referenced above.

6.2.3.1.4 Back-out procedures

PCI DSS Requirement 6.4.5.4 – Back-out procedures

Refer to PCI DSS Requirement 6.4.5 policies and procedures referenced above.

6.2.4 Address common code vulnerabilities

PCI DSS Requirement 6.5 - 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.

Policy: We address common coding vulnerabilities in the software-development process by:

- ensuring developers are trained in secure coding techniques
- developing applications based on secure coding guidelines as defined in PCI DSS Requirements 6.5.1, 6.5.2, 6.5.7, 6.5.8, 6.5.9, and 6.5.

Procedure:

- Develop, implement, and disseminate secure coding guidelines.
- Train developers in secure coding techniques.
- Employ application testing methods to ensure that secure coding techniques have been utilized.
- Develop relationships with industry organizations and standards bodies in order to maintain an ongoing awareness of new coding techniques that can prevent coding vulnerabilities.

6.2.4.1 Injection flaws

PCI DSS Requirement 6.5.1 - Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent injection flaws related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent injection flaw vulnerabilties by:

- defining and using secure coding standards and practices.
- using software coding techniques that:
  - validate input to verify user data cannot modify meaning of commands and queries.
  - utilize parameterized queries.
- training of our personnel in secure coding techniques.
- through testing procedures that verify that securing coding practices have been used.
- maintain ongoing awarness of newly discovered injection flaw related vulnerability prevention techniques from industry recognized third parties and standards bodies.

6.2.4.2 Buffer overflow

PCI DSS Requirement 6.5.2 - Buffer overflow

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent buffer overflow related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent buffer overflow vulnerabilities by:

- defining and using secure coding standards and practices.
- using software coding techniques that include:
  - validating buffer boundaries.
  - truncating input strings.
- training of our personnel in secure coding techniques.
- through testing procedures that verify secure coding practices have been used.
- maintain ongoing awarness of newly discovered buffer overflow related vulnerability prevention techniques from industry recognized third parties and standards bodies.

6.2.4.3 Cross-site scripting (XSS)

PCI DSS Requirement 6.5.7 - Cross-site scripting (XSS)

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent cross-site scripting (XSS) related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent cross-site scripting (XSS) vulnerabilities by:

- defining and using secure coding standards and practices.
- using software coding techniques that include:
  - validating all parameters before inclusion.
  - utilizing context-sensitive escaping.
- training of our personnel in secure coding techniques.
- through testing procedures that verify secure coding practices have been used.
- maintain ongoing awarness of newly discovered cross-site scripting (XSS) related vulnerability prevention techniques from industry recognized third parties and standards bodies.

6.2.4.4 Improper access control

PCI DSS Requirement 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).

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent improper access control related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent improper access control vulnerabilities by:

- defining and using secure coding standards and practices.

- preventing improper access control such as insecure direct object references, failure to restrict URL access, and directory traversal through the use of software coding techniques that include:
    - proper authentication of users.
    - sanitizing input.
    - not exposing internal object references to users.
    - user interfaces that do not permit access to unauthorized functions.
- training of our personnel in secure coding techniques.
- through testing procedures that verify secure coding practices have been used.
- maintain ongoing awarness of newly discovered improper access control related vulnerability prevention techniques from industry recognized third parties and standards bodies.

6.2.4.5 Cross-site request forgery

PCI DSS Requirement 6.5.9 – Cross-site request forgery

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent cross-site request forgery (CSRF) related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent CSRF vulnerabilities by:

- defining and using secure coding standards and practices
- using software coding techniques that ensure applications do not rely on:
    - authorization credentials.
    - tokens automatically submitted by browsers.
- training of our personnel in secure coding techniques.
- through testing procedures that verify secure coding practices have been used.
- maintain ongoing awarness of newly discovered CSRF related vulnerability prevention techniques from industry recognized third parties and standards bodies.

6.2.4.6 Broken authentication and session management

PCI DSS Requirement 6. 5.10 – Broken authentication and session management.

Policy: We use industry best practices to produce software code for our applications used within the cardholder data environment to prevent broken authentication and session management related vulnerabilities.

Procedure: We ensure secure coding practices are used to prevent broken authentication and session management vulnerabilities by:

- defining and using secure coding standards and practices.
- using software coding techniques that address broken authentication and session management to prevent malicious individuals from compromising legitimate account credentials, keys or session tokens.
- training of our personnel in secure coding techniques.
- through testing procedures that verify secure coding practices have been used.
- maintain ongoing awareness of newly discovered broken authentication and session management related vulnerability prevention techniques from industry recognized third parties and standards bodies.

PCI DSS Requirement 6.6 - 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.
* By an organization that specializes in application security
* That all vulnerabilities are corrected
* That the application is re-evaluated after the corrections

Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.

OR

* Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

Policy:

- We ensure that public-facing web applications are protected:
  - against new threats.
  - from vulnerabilities on an ongoing basis by reviewing public-facing web applications via automated application vulnerability security assessment tools .
- We perform these reviews either:
  - at least annually .
  - after any system component or application changes .
- An organization that specializes in application security is used to peform the review.
- All identified vulnerabilities are corrected .
- System component(s) and application(s) security is re-evaluated after corrections are applied.

Procedure: We will use automated software data collection and report analysis to identify and review all the public facing system components and applications to ensure that the appropriate vendor-provided patches are installed to protect the cardholder data environment

7 Implement Strong Access Control Measures

7.1 Restricted access to cardholder data

PCI DSS Requirement 7 - Restrict access to cardholder data by business need-to-know

Policy: Members of the workforce are to be granted access only to that Cardholder Data to which they are authorized in order to perform their job role or associated job function. All members of the workforce will be trained regarding appropriate access to Cardholder Data, including the awareness of information access controls. Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to Cardholder Data. We will develop security policies to identify core activities in the areas of access authorization, access establishment and modification.

Procedure: This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in our plan (see Procedures related to monitoring audit logs, access reports and security incident tracking). Workforce should be trained to never access Cardholder Data using another person's credentials, including on a system left logged in by someone else. End users should be familiar with the Sanction Policy and know what to expect if they violate rules.

7.1.1 Limit access to system components and cardholder data

PCI DSS Requirement 7.1 - Limit access to system components and cardholder data to only those individuals whose job requires such access.

Policy: Members of the workforce (cardholder data environment users and administrators) are to be granted access only to the cardholder data and system components to which they are authorized in order to perform their job role or associated job function.

All members of the workforce will be trained regarding appropriate access to cardholder data and system components, including the awareness of information access controls.

Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to cardholder data and system components.

We will develop security policies to identify core activities in the areas of cardholder data environment and system component access authorization, access establishment and modification.

Procedure: Access to system components and cardholder data limited to only those individuals whose jobs require such access, as detailed in PCI DSS Requirements 7.1.2 and 7.1.3 detailed below.
We will use automated software data collection and report analysis to identify and review all logins to system components and applications to ensure that:

- users are accessing applications and system components using IDs that have been authorized to do so
- to ensure that generic IDs have not been issued to enable access to cardholder data or system components

- to verify that user access mechanisms are configured to operate in a fashion that adheres to the guidelines above.

Training Considerations: Workforce should be trained to never access cardholder data or system components using another person's credentials, including on a system left logged in by someone else. End users should be familiar with the Sanction Policy and know what to expect if they violate rules.

7.1.1.1 Limit access to system components and cardholder data

PCI DSS Requirement 7.1.2 - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

Policy: This policy is about workforce users' and/or system administrator users' right of access to cardholder data and system components. The individual's job description must be reviewed to determine their:

- workforce personnel's job role and responsibilities
- individual rights
- the group that this individual belongs to
- the principle of least privilege that influences the cardholder data and/or system component's access rights granted to an individual or a third party
- business need
- access must be granted only to roles based that specifically require privileged access

Procedure: To validate that access policies are being followed, we will generate regular monthly reports to determine if generic accounts are used which do not support logging individual's access to cardholder data or system components. We will also review and determine what privileged/administrator users have not logged into the system as an indicator that their work is being delegated to others or that they are 'piggy-backing' on another user's login.

7.1.1.2 Assign access based on individual personnel's job classification and function

PCI DSS Requirements 7.1.3 - Assign access based on individual personnel's job classification and function.

Policy: Cardholder data environment and system component access rights and privileges are granted to workforce users upon the user's role and job function within the entity.

Procedure: To validate that access policies are being followed, we will generate regular monthly reports to determine if generic accounts are used which do not support logging individual's access to cardholder data or system components.

As a part of this process, periodic reviews of users' job functions versus their assigned access rights and privileges to the cardholder data environment and system components will be examined to ensure that the "least privileges" have been assigned to the user based on their current job function.
We will also review and determine what workforce users and administrator users have not logged into the system as an indicator that their work is being delegated to others or that they are 'piggy-backing' on another user's login.

7.2 Access to Cardholder Data Environment (CDE) system components

PCI DSS Requirement 8 - Identify and authenticate access to system components

Policy: We use best practices and have implemented industry accepted guidelines to ensure that all users that access the cardholder data environment and system components are uniquely accountable for their accounts and that all activity on critical data and systems can be traced to know and authorized users.

Procedure: Each individual that accesses system components will be assigned a unique user ID. An authentication system has been implemented to ensure the effectiveness of passwords by protecting that user passwords at the point of entry, during transmission, and while in storage while monitoring the number of attempts are made to use a password for a given user account logon.

To monitor this policy's effectiveness and to identify potential attempts by malicious users to penetrate the cardholder data environment and/or system components, on a monthly basis a report will be generated containing all information logged for both successful and failed user logon access attempts.

7.2.1 Proper User Identification Management for Non-Consumer Users and Administrators

PCI DSS Requirement 8.1 - Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components a

Policy: We have defined and implemented policies and procedures to ensure proper user identification management for non-consumer and administrators on all system components consistent with the PCI DSS Requirements 8.1.1, 8.1.3, 8.1.5, 8.1.6, and 8.1.7. These policies and procedures have been implemented to ensure that user action responsibility and effective audit trails can be monitored and maintained.

Procedure: The policies and procedures for PCI DSS Requirements 8.1.1, 8.1.3, 8.1.5, 8.1.6, and 8.1.7 to ensure proper users identification management for non-consumer and administrators on all system components are detailed below in the following sections.

7.2.1.1 Unique User Identification

PCI DSS Requirement 8.1.1 - Assign all users a unique ID before allowing them to access system components or cardholder data.

Policy: Each individual that accesses sensitive information, such as system components and/or cardholder data, via computer at work will be granted some form of unique user identification such as a login ID. At no time will any workforce user allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else's ID. We will:

- develop a standard convention for assigning unique user identifiers.
- maintain a secure record of unique user identifiers assigned.
- track individual activities and record events as required by policies such as Audit and Information System Activity Review.

Procedure: To validate that access policies are being followed, regularly review user login reports to determine if generic accounts are used which do not support logging individual's access to system components and cardholder data. Also determine which users have not logged into the system as an indicator that their work is being delegated to others or that they are 'piggy-backing' on another user's login.

Training Considerations: Work staff should be trained to never access cardholder data using generic passwords; logging in as someone else; or accessing a system left logged in by someone else. Staff should be familiar with the Sanction Policy and know what to expect if the rules are violated.

7.2.1.2 Termination Procedures

PCI DSS Requirement 8.1.3 - Immediately revoke access for any terminated users.

Policy: People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments quickly coordinating their activities to ensure:

- password access is immediately revoked
- access to all systems and applications is revoked
- the workforce member is removed from any systems or applications that process Cardholder Data and/or system component administration permissions
- all digital certificates are revoked
- any tokens or smart cards issued to the workforce member are returned
- any keys and IDs provided to the workforce member during their employment are returned
- the workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised If the workforce member might know other worker's passwords, they should be changed immediately
- HR must conduct an exit interview and document any issues or concerns related to the workforce member

Procedure: When an employee that has performed job duties within the cardholder data environment is terminated:

- validate that terminated employees are no longer on the active user list
- review the Security Assessment report with HR to identify users that may still have access to Cardholder Data but are either no longer with the organization or have a business relationship requiring access.
- determine if generic accounts are used which do not support logging individual's access to Cardholder Data.
- remember to check all systems and online services that contain Cardholder Data.

7.2.1.3 Third-Party User ID Management, System Component Access, and Monitoring

PCI DSS Requirement 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.

Policy: All user IDs and accounts provided to third-parties to access, support, or maintain system components via remote access are to be disabled when not in use. During a third-party user's access of the system components, we will monitor third-party access activity to ensure that the third-party user is accessing only the systems necessary and only during approved time frames.

Procedure: System administrators are to be notified in advance of third-party requirements to access system components remotely. Administrators will coordinate with the third-party to activate the user account and ID to enable remote access. When the third-party ID is activated, the administrator will ensure that all third-party access to system components is monitored by a member of our organization's workforce until the third-party's user ID is disabled.

7.2.1.4 Repeated login access attempts

PCI DSS Requirement 8.1.6 - Limit repeated access attempts by locking out the user ID after not more than six attempts.

Policy: Our established user ID configuration practices require that all applications and system components are configured to limit repeated failed access attempts by locking out the user ID after six (6) failed login attempts.

Procedure: System components and applications will be configured to lockout the user ID after no more than six (6) login attempts.

On a monthly basis a report will be generated containing all information logged for both successful and failed user logon access attempts in order to monitor this policy's effectiveness and to identify potential attempts by malicious users to penetrate the cardholder data environment and/or system components.

7.2.1.5 User ID lockout duration

PCI DSS Requirement 8.1.7 - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

Policy: Our established application and system component configuration standards require that the user ID lockout duration be set to a minimum of 30 minutes or until an administrator enables the user ID.

Procedure: We will use automated software data collection and report analysis to identify and review all user ID configuration parameters to ensure that the lockout duration mechanism is set and maintained in compliance with the guidelines above.

7.2.2 Ensuring proper user-authentication management

PCI DSS Requirement 8.2 - 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.

Policy: We recognize that the use of passwords as an authentication method is inherently insecure and require the use of strong authentication solutions for non-consumer users and administrators of all system components.

Strong authentication solutions use a combination of two or more factors (described above) when granting or denying access; such as the presence of a fingerprint (something the user is) combined with a pin number (something the user knows).

We will evaluate emerging strong authentication technologies on a periodic basis and implement them when one is found that is:

- Technically sound and useable
- Financially reasonable
- Meets business objectives

We will give strong authentication preference to users who pose a higher risk to the organization. High risk users include (but are not limited to):

- Users that have administrator rights to systems that contain sensitive information
- Users that connect to the network remotely
- Users that have portable computing devices such as laptops or PDAs that may be carried off the premises

Procedure: Use automated software and reporting to determine that user passwords meet the criteria described above and review violations with the users and report incidents to the security officer.

7.2.2.1 Encryption of all authentication credentials

PCI DSS Requirement 8.2.1 - Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Policy: Our system component configuration standards and best practices implementation require that all authentication credentials, such as password/passphrases are rendered unreadable during transmission and storage using strong cryptography on all system components within the cardholder data environment.

Procedure: Acquire only system components from third parties that can ensure that the components use strong cryptography to render password/passphrases unreadable during storage and transmission.

Use our configuration standards and guidelines to ensure that system components placed within the cardholder data environment are implemented with features activated that render the password/passphrases in storage and transmission unreadable using strong encryption.

Use automated software and reporting to determine that system component configurations enable/render user passwords to meet the criteria described above and review violations with the system component administrators and report incidents to the Cardholder Data Security Officer.

7.2.2.2 Password strength and complexity

PCI DSS Requirement 8.2.3 - Passwords/phrases must meet the following:

* Require a minimum length of at least seven characters.
* Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

Policy: All workforce members that use passwords/passphrases will make efforts to keep those passwords/passphrases safe and secure. At no time will any workforce member:

- write down their passwords/passphrases, either on paper or in an electronic file
- share or otherwise disclose their passwords/passphrases to anyone else for any reason including technical support, managers, and supervisors
- keep the same passwords/passphrases for longer than 90 days
- use a passwords/passphrases that is the same as or a variation of any passwords/passphrases has been used before
- use the "remember password" option on any program that supplies the passwords/passphrases for the user
- use a "weak" password as described below

Weak passwords will not be used for any reason. Weak passwords have the following characteristics:

- contain less than seven (7) characters
- do not contain both numeric and alphabetic characters
- a word found in a dictionary (English or foreign)
- common usage word such as:
- names of family, pets, friends, co-workers, fantasy characters, and so on
- computer terms and names, commands, sites, companies, hardware, software
- birthdays and other personal information such as addresses and phone numbers
- word and/or number patters like aaabbb, qwerty, zyxwvuts, 123321, and so on
- any of the above spelled backwards
- any of the above preceded or followed by a digit (for example, secret1, 1secret)

If a passwords/passphrases is suspected to have been compromised (or if anyone requests or demands a passwords/passphrases), it shall be treated as a security incident and reported to the Cardholder Data Security Officer.

Procedure: Use automated software and reporting to determine that user passwords/passphrases meet the criteria described above and review violations with the users and report incidents to the Cardholder Data Security Officer.

At a minimum, system configuration settings to must be verified to ensure that user password parameters are set to require at least the following strength/complexity:
* Require a minimum length of at least seven characters.
* Contain both numeric and alphabetic characters.

7.2.2.3 Password expiration policy

PCI DSS Requirement 8.2.4 - Change user passwords/passphrases at least every 90 days.

Policy: All workforce members that use passwords/passphrases will make efforts to keep those passwords/passphrases safe and secure.

At no time will any workforce member have a password/passphrase that is older than 90 days.

Procedure: Use automated software and reporting to determine that user passwords/passphrases meet the criteria described above.

7.2.2.4 New password/phrase requirements

PCI DSS Requirement 8.2.5 - Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

Policy: When any individual submits a new password/passphrase, they are prohibited from submitting a new password/passphrases that is the same as the last four passwords/passphrases he or she has used in the past.

Procedure: In system components and applications within the cardholder data environment that support the tracking of user ID/account password/passphrase histories, individuals will be automatically prevented from using the same password/passphrase as one of the last four passwords/passphrases used.
In the case that automatic prevention measures cannot be implemented or relied upon, system administrators are to remind users of this policy during the process of an individual user requesting a new password/passphrase.

System component administrators, network support personnel, and individual users will also be made aware of this policy through training, continuing education, email newsletters, and other communications methods to ensure they are aware of policy when requesting new passwords/passphrases.

7.2.2.5 Password/phrase first-time use and reset requirements

PCI DSS Requirement 8.2.6 - Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

Policy: We recognized that if the same password is used for every new user that an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts. We have implemented a policy and system component/application technology configuration whereby:

- first-time passwords must be set to a unique value for each user
- first-time passwords must be changed after the first use
- reset passwords must be set to a unique value for each user
- reset passwords must be changed after the first use

Procedure: All passwords/phrases are to be set to a unique value for each user for first-time use and upon reset, the system must prompt each user change their password immediately after the first use.

7.2.3 Multi-Factor authentication requirement for remote network access by users

PCI DSS Requirements 8.3.2 - Incorporate multi-factor authentication for remote network access originating from outside the network, by personnel (including users and administrators) and all third parties, (including third-party access for support or maintenance).

Policy: It is policy that multi-factor authentication is employed to manage higher risk access which includes remote user access to the network by general users, administrators, and third-parties (for support or maintenance) with remote access rights to the networks that have access to the cardholder data environment(s).

Procedure: Multi-factor authentication has been incorporated into the network to provide for remote network access originating from outside our organization's network by personnel (including users and administrators) and all third parties (including third-party access for support or maintenance).

The multi-factor authentication technologies implemented for remote access to the cardholder data enviroment includes one or more of the following:

- remote authentication and dial-in service (RADIUS) with tokens
- terminal access controller access control system (TACACS) with tokens
- other technologies that facilitate multi-factor authentication.

7.2.4 Group, shared, and Generic IDs prohibition policy

PCI DSS Requirement 8.5 - 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.

Policy: We recognize the need to fully account for local and remote user access to the Cardholder Data Environment (CDE) and/or cardholder data on a per user basis.

The need to account for user access includes the requirement to ensure that individual workforce users and third-party users are assigned specific user IDs and accounts to enable access to applications and/or system components for business and/or maintenance uses.

Our processes used to request, approved and generate user IDs strictly prohibits the creation and use of group, shared or generic IDs and passwords to access system components within the Cardholder Data Environment.

The use of group, shared, or generic IDs, passwords to access system components within the Cardholder Data Environment and/or card holder data are forbidden.
Workforce users are trained in the above mentioned policy and are required to report any suspect login credentials that appear to be inconsistent with the aforementioned policy.

Procedure: We ensure that:

A) generic user IDs are disabled or removed.
B) shared user IDs do not exist for system administration and other critical functions.

C) shared and generic user IDs are not used to administer any system components.

Training Considerations: Workforce users that receive authorization to access the cardholder data environment are trained in the policy outlined above.

7.2.5 Authentication mechanism use assignments

PCI DSS Requirement 8.6 - 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.

Policy: Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), the use of these mechanisms is assigned as follows:

- authentication mechanisms are assigned to an individual account
- authentical mechanisms are not shared among multiple accounts
- physical and/or logical controls and safeguards such as Biometric data (something a person is), or a PIN/password (something a person knows) must be in place to ensure only the intended account can use that mechanism to gain access

Procedure: The assignment of other authentication mechanisms to users and administrators is to be formally requested, authorized, and logged. Upon user termination from employment, any physical devices storing security tokens and/or smart cards are to be secured from the user by Human Resources department consistent with established security policy.

Training consideration: Non-consumer users and administrators are to be trained on the policies concerning the prohibition of sharing user ID, password and authentication mechanisms with other users and the associated sanctioning policies for the failure to comply with the policy detailed above.

7.3 Controlling physical access to cardholder data

PCI DSS Requirement 9. Restrict physical access to cardholder data

Policy: We restrict physical access to cardholder data by:

- controlling physical access to all computer rooms, data centers, and other physical areas with systems in the cardholder data environment
- requiring that all users lock consoles for systems in the cardholder environment after each use
- requiring personnel place all hardcopies of cardholder data under “lock and key” immediately following use

Procedure: Access to computer rooms, data centers, and physical areas with systems in the cardholder data environment can only be accessed by “on-site personnel” using either:

- authorized badges read by badge readers that operate door controls

- door lock keys

"On-site personnel" is defined to mean full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises.
All cardholder environment users are trained to lock their consoles accessing the cardholder data environment after use. Periodic monitoring of consoles is used to ensure that users comply with this policy.
All users of hard copy documents containing cardholder data are trained to ensure that they place all hard copies of these documents under "lock and key" when not in use.

Periodic monitoring of the presence of hard copy information in common area work locations is performed to ensure that this procedure is being followed. Locations inspected include:

- user work areas
- network printer locations operating within the cardholder data environment
- fax machine locations

7.3.1 Facility entry controls and monitoring physical access to systems in the cardholder data environment

PCI DSS Requirement 9.1 - Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

Policy: We control physical access to all computer rooms, data centers, and other physical areas with systems in the cardholder data environment

Procedure: Access to computer rooms, data centers, and physical areas with systems in the cardholder data environment can only be accessed by "on-site personnel" using either:

- authorized badges read by badge readers that operate door controls
- door lock keys

7.3.2 Physically securing all media

PCI DSS Requirement 9.5 - Physically secure all media.

Policy: We physically secure all media containing cardholder data by requiring:

- that all users lock consoles for systems in the cardholder environment after each use or automatic log-off solutions are implemented to log the systems out
- personnel place all hardcopies of cardholder data under "lock and key" immediately following use
- that removable storage media is stored under "lock and key" immediately following use

Procedure: All cardholder environment users' consoles are set to automatically lock after a period of time. Users are also required to immedially lock their consoles used for accessing the cardholder data environment after each use. Periodic monitoring of consoles is used to ensure that users comply with this policy.
All users of hard copy documents and removable storage media containing cardholder data are trained to ensure that they place all hard copies of these documents under "lock and key" when not in use.

Periodic monitoring of the presence of hard copy information in common area work locations is performed to ensure that this procedure is being followed. Locations inspected include:

- user work areas
- network printer locations operating within the cardholder data environment
- fax machine locations

7.3.3 Controls over internal and external distribution of any kind of media

PCI DSS Requirement 9.6 - Maintain strict control over the internal or external distribution of any kind of media, including the following:

Policy: We strictly control the internal and external distribution of any kind of media through ensuring that:

- we classify the media based upon the sensitivity of the data stored on the media
- we use a secure courier or other delivery method where the media is tracked
- management is fully aware that the media has been requested and management approves the distribution and/or moving of the media

Procedure:

- Only transport the media externally using a secured courier or other delivery method whereby the media is accurately tracked.
- Request and secure authorization from the organization's management before the media is distributed to an individual.
- Ensure that the use of strong cryptography is employed encrypt data stored on all electronic media in order to prevent malicious individuals from being able to view, alter, or use the data.

7.3.3.1 Media classification to determine sensitivity

PCI DSS Requirements 9.6.1 - Classify media so the sensitivity of the data can be determined.

Policy: We classify the media based upon the sensitivity of the data stored on the media.

Procedure:

- Use standard industry practices to classify media based upon the sensitively of the data stored on it.
- Identify the media referencing the classification of the data stored on the media in order to ensure that individuals within the organization can easily determine what level of protection and care should be employed when handling and transporting the media.
- Log the media's classification in all media storage inventory records.

7.3.3.2 Send media by secured courier or other delivery method that can be tracked

PCI DSS Requirement 9.6.2 - Send the media by secured courier or other delivery method that can be accurately tracked.

Policy: We send media by secured courier or via other delivery methods that can be easily tracked.
Procedure:

- Send media only by secured couriers and/or other delivery methods whereby the media can be easily tracked by the organization.
- Only reputable secured courier and delivery firms that are authorized by the organization are to be used for distributing/shipping media.
- All media sent outside the facility is to be logged and the delivery of the media followed up on to ensure the media was delivered to the intended recipient and was not tampered with during transit.

7.3.3.3 Management notification and approval of all media moved from a secured area

PCI DSS Requirement 9.6.3 - Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).

Policy: Prior to the movement of media held in a secured area (including when media is distributed to individuals), approval from management must be obtained. This policy applies to any and all media.

Procedure: The procedure to move media held in a secure area is as follows:

- Prepare a request for the media to be distributed to a new location or to an individual.
- Submit the request to management.
- Secure management approval.
- Log management approval of the media movement request.
- Release the media for distribution.
- Log the movement of the media and reference the location and/or individual that is to receive the media in the offsite media tracking log.
- Log receipt of the media at the new location or by an individual.

7.3.4 Maintain strict control over media storage and accessibility

PCI DSS Requirement 9.7 - Maintain strict control over the storage and accessibility of media.

Policy: All stored media containing cardholder data is stored in a secure storage area. All stored media's physical location within the storage area(s) is documented and tracked for inventory purposes.

Procedure: All media that is to be placed in storage is to:

- be logged and inventoried prior to being placed into the secure storage location.
- undergo periodic media inventory reviews to ensure that the whereabouts of all media placed into storage areas is monitored.
- be authorized by management for access or movement prior to access to the media being granted.
- any movements of the media must be logged.

7.3.5 Media destruction policy

PCI DSS Requirement 9.8 - Destroy media when it is no longer needed for business or legal reasons as follows:

Policy: It is our policy to ensure that information, including cardholder data, stored on media is held in secure locations at all times. Once this media is no longer needed for business or legal reasons the media is:

- retrieved from its secure location
- stored in containers that are secured at all times
- in the case of hard copy media, destroyed using techniques that ensure that malicious individuals cannot reconstruct card holder data from the destroyed media fragments
- in the case of electronic media, cardholder data on the media must be rendered unrecoverable in accordance with industry- accepted standards for secure deletion or physical destruction

Procedure: Once media is no longer needed for business or legal reasons, the media is:

- stored in a secure location until it is retrieved for destruction by internal personnel or an authorized third party. Such locations may include a “to-be-shredded” container that is locked and secure.
- destroyed using techniques that ensure that cardholder data cannot be reconstructed. Destruction techniques may include crosscut shredding, incineration, or pulping (for hard-copy paper media) and in the case of electronic media secure wiping, degaussing, or physical destruction using grinding or hard disk shredding.

8 Regularly Monitor and Test Networks

8.1 Track and monitor access to network resources and cardholder data

PCI DSS Requirement 10 - Track and monitor all access to network resources and cardholder data

Policy: We will ensure that all system components have automated audit trail logging capabilities. We will define the events to be audited on all such systems. At a minimum, event auditing capabilities will be enabled on all systems that process, transmit, and/or store cardholder data and include audit trail logging of all access to system components by system administrators and other personnel and third parties with access rights.

Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications, and system component configuration modifications. We will ensure the protection and retention of all audit trail reports and log files in compliance with PCI DSS requirement 10.7.

We will review the usage of software and application tools to review audit trail files at intervals specified by PCI DSS requirement 10.6. When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of the security team. This access may include:

- User level and/or system level access to any computing or communications device
- Access to cardholder data that may be produced, transmitted, or stored on system components and equipment, hosted service, or remote location
- Access to work areas (offices, cubicles, storage areas, and so on) where system components or systems accessing cardholder data environment exist
- Access to interactively monitor and log traffic on our networks

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on, to ensure audit trail files and logs are stored, and review reports generated monthly.

8.1.1 Automated audit trails for all system components

PCI DSS Requirement 10.2 - Implement automated audit trails for all system components to reconstruct the following events:

Event	PCI DSS Requirement
All actions taken by any individual with root or administrative privileges	10.2.2
Invalid logical access attempts	10.2.4
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	10.2.5

Policy: Consistent with industry best security practices to track and monitor activity within the cardholder data environment we have implemented audit trails for all system components to reconstruct events specified in and PCI DSS Self Assessment Questionnaire (SAQ) A-EP requirements 10.2.2, 10.2.4, and 10.2.5 detailed above. These audit trails are used to reconstruct above referenced events in the case of a suspicious activity or as part of a periodic review of audit trails consistent with our security readiness review practices.

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on, to ensure audit trail files and logs are stored, and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.1.1 Generate audit trail of all actions taken by any individual with root or administrative privileges

PCI DSS Requirement 10.2.2 - All actions taken by any individual with root or administrative privileges.

Policy: Consistent with industry best security practices to track and monitor activity within the cardholder data environment, we have implemented audit trails for all system components to reconstruct events associated with all actions taken by any individual with root or administrative privileges. These audit trails are used to reconstruct above referenced events in the case of a suspicious activity or as part of a periodic review of audit trails consistent with our security readiness review practices.

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on, to ensure audit trail files and logs are stored, and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.1.2 Generate audit trails of invalid logical access attempts

PCI DSS Requirement 10.2.4 - Invalid logical access attempts.

Policy: Consistent with industry best security practices to track and monitor activity within the cardholder data environment we have implemented audit trails for all system components to reconstruct events associated with invalid logical access attempts.
These audit trails are used to reconstruct above referenced events in the case of a suspicious activity or as part of a periodic review of audit trails consistent with our security readiness review practices.

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on, to ensure audit trail files and logs are stored, and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.1.3 Generate audit trails of the use of and changes to identification and authentication mechanisms

PCI DSS Requirement 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.

Policy: Consistent with industry best security practices to track and monitor activity within the cardholder data environment we have implemented audit trails for all system components to reconstruct events associated with use of and changes to identification and authentication mechanisms–including but not limited to:

- creation of new accounts
- elevation of privileges
- all changes, additions, or deletions to accounts with root or administrative privileges.

These audit trails are used to reconstruct above referenced events in the case of a suspicious activity or as part of a periodic review of audit trails consistent with our security readiness review practices.

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on, to ensure audit trail files and logs are stored, and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.2 Recording audit trail entries for all system components for each event

PCI DSS Requirement 10.3 - Record at least the following audit trail entries for all system components for each event: (below)

Event	PCI DSS Requirement
User identification	10.3.1
Type of event	10.3.2
Date and time	10.3.3
Success or failure indication	10.3.4
Origination of event	10.3.5
Identity or name of affected data, system component, or resource	10.3.6

Policy: Consistent with industry best security practices to track and monitor activity within the cardholder data environment we record the audit trail entries listed above for all system component for each of the auditable events detailed in PCI DSS Requirements 10.2.

Procedure: We will use automated software data collection and report analysis to validate that logging system components' configurations enable the recording of these entries and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.3 Securing audit trails to prevent alteration

PCI DSS Requirement 10.5 - Secure audit trails so they cannot be altered.

Policy: We shall secure audit trails so that they cannot be altered to ensure their integrity in support of our audit trail monitoring and review policies.

Procedure: We will use automated software data collection and report analysis to collect information from system components in order to validate that audit trails are secure and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.3.1 Write logs for external-facing technologies on a secure log server or media device

PCI DSS Requirement 10.5.4 - Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

Policy: In accordance with our system component configuration standards, we configure the system components that operate external facing technologies to write logs onto a secure, centralized, internal log server and/or media device. External facing technologies may include, but are not limited to, wireless networks, firewalls, DNS, and electronic mail.

Procedure: We will use automated software data collection and report analysis to collect information from system components in order to validate that system components for external facing technologies write logs to a

centralized internal log server or media device and review reports generated monthly in compliance with the policy and practices outlined above.

8.1.4 Review logs and security events for all system components

PCI DSS Requirement 10.6 - Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.

Policy: Our security policy and practices require that logs and security events for all system components are reviewed by personnel training in identifying anomalies and suspicious activity within the cardholder data environment and its system components within the environment.

Procedure: On a daily basis we review logs and security events for all system components. During this review process we review event data and search for anomalies and any event that is suspicious in its nature.

8.1.4.1 Daily review of security events including logs of system components, critical system components, and servers that perform security functions

PCI DSS Requirement 10.6.1.b - Review the following at least daily: * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of 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.).

Policy: Our security policy requires that stringent efforts be undertaken to monitor for and identify anomalies and suspicious activity within the cardholder data environment and its system components within the environment to identify potential instances of malicious activity.

Procedure: On a daily basis we review:

- all security events
- logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD

(Please note: The acronym CHD stands for Cardholder Data, the acronym SAD stands for 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.)

During this review process we review event data and search for anomalies and any event that is suspicious in its nature and report any anomalies and suspicious events.

8.1.4.2 Review logs of all other system components periodically based on risk management strategy and annual risk assessment

PCI DSS Requirement 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.

Policy: We periodically examine the logs of system components that fall outside of the purview of the system components referenced in 10.6.1.b (defined as less sensitive systems) based on the intervals set forth in the organization's risk assessment strategy and annual risk assessment.

Procedure: The **20YY** annual risk assessment states that the logs for these system components should be examined every **XX** days. This procedure will be updated within **XX** days after each annual risk assessment. On a (**monthly, quarterly or yearly – select one)** basis we examine the organization's most recent risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.

8.1.4.3 Follow up exceptions and anomalies identified during the review process

PCI DSS Requirement 10.6.3 - Follow up exceptions and anomalies identified during the review process.

Policy: In compliance with security risk management guidelines and audit practices, upon the identification of any exceptions and/or anomalies identified during the review of security events, logs and audit trails, the following actions are taken:

- the Cardholder Data Security Officer is notified
- risk assessment/forensic processes are initiated

Procedure: Upon the identification of exceptions and/or anomalies and the notification of the Cardholder Data Security Officer, all audit trails and logs are verified to be secured, and backed-up while the Cardholder Data Security Team awaits a security assessment and action plan to act upon in response to the identified exceptions and/or anomalies.

8.1.5 Retain audit trail history

PCI DSS Requirement 10.7 - 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).

Policy: In compliance with security risk management guidelines and audit practices to enable potential breach identification and system impact, we:

- retain system component audit trail history for a minimum period of one year
- at all times, we have a three month history is immediately available for review and analysis.

Procedure: We will use automated software data collection and report analysis to collect information from system components in order to validate that audit trails are being produced and that historical audit trails are being centrally stored in a secure location in compliance with the policy and practices outlined above.

8.2 Regular testing of security systems and processes

PCI DSS Requirement 11 - Regularly test security systems and processes

Policy: We regularly test security systems and processes using:

- external vulnerability scans
- internal vulnerability scans
- penetration testing methodologies and test performance
- methods that enable testing of segmented networks
- change-detection mechanisms

Procedure:

- perform an external vulnerability scan quarterly or after a significant change to the cardholder data environment
- perform an internal vulnerability scan quarterly or after a significant change to the cardholder data environment
- perform penetration tests annually or after a significant change to the cardholder data environment
- perform penetration tests on segmented networks to ensure they are operational and effective and that out-of-scope and in-scope operation is performing as designed and securely
- respond to alerts issued by the change-detection mechanism

8.2.1.1 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC)

PCI DSS Requirement 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.

Policy: In an effort to prevent and eliminate security vulnerabilities, we employ a PCI SSC Approved Scanning Vendor (ASV) to perform quarterly external vulnerability scans on the cardholder data environment. External scans and rescan results performed must satisfy the PCI DSS ASV program guide requirements for passing a scan, which includes that no vulnerabilities rated at 4.0 or higher by the CVSS, and no automatic failures.

Procedures: External vulnerability scans are performed on a quarterly basis. All vulnerabilities rated at 4.0 or higher by the CVSS must be immediately eliminated.
All initial external scan reports, automatic failure reports, and rescan reports must be submitted to the internal PCI DSS Security Officer for review, sign-off, and recording.

8.2.1.2 Perform internal and external scans, and rescans as needed, after any significant change

PCI DSS Requirement 11.2.3 - Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

Policy: As a part of our Risk Management strategy, we have determined that "significant change" means any updated or modification to the cardholder data environment whereby the modification could allow access to cardholder data or affect security of the cardholder data environment.
Any time there is a "significant change" is made to the cardholder data environment system components and/or applications, the final change will be accepted and placed into operation after an internal and external scan (and necessary rescans) have been performed to ensure that the cardholder data environment has no unresolved security issues/vulnerabilities:

- at a CVSS 4.0 rating for "external facing" system components
- defined as "high risk" vulnerabilities as specified in PCI DSS Requirement 6.1 for all "internal" system components

These scans must be performed by qualified personnel, or a qualified third party.

Procedure: We will use automated software data collection and report analysis to perform scans of cardholder data environment system components and review all services implemented on systems and ensure that the system components' configurations adhere to the guidelines to safeguard cardholder data during transmission.

All scan reports must correlate to system component change control documentation.

All initial external/internal scan reports, automatic failure reports, and rescan reports must be submitted to the internal Cardholder Data Security Officer for review, sign-off, and recording prior to approving cardholder data environment for use.

PCI DSS Requirement 11.2.3.a – Internal and external scans, and rescans as needed, performed after any significant change.

Policy: All internal and external system component scans, and rescans as needed, will be peformed performed upon system components after any significant change. Scans will be performed by qualified personnel.

Procedure: After any signification changes have been made to one or more system components, the Cardholder Data Security Officer must ensure that:

- System component change control documentation has been coorelated with component scan reports to ensure that the scan reports verify that any components subject to a significant change have been scanned.
- Verify that any system component that did not initially meet acceptable security standards tested with the scanning process were rescanned until the system componment meet the acceptance security criteria.
- All scan documentation is retained for future reference in compliance with the associated policies.

PCI DSS Requirement 11.2.3.b – Scan process includes rescans until external and internal scans until vulnerability standards are met

Policy: Our system component scan process includes rescans until external and internal scan vulnerability standards are met.

Procedure: External and internal system components are scanned and rescan for vulnerabilities until:

- For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS.
- For internal scans, all "high- risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.

PCI DSS Requirement 11.2.3.c – Scans are to be performed by a qualified internal resource or a qualified external third party, and if applicable, organization independence of the tester exists (not required to be a QSA or ASV).

Policy: Scans after significant changes are performed:

- by qualified internal resources or qualified third parties
- by a party whereby the scan tester is organizationally independent from the organization that made the significant change to the system components

Procedure: After each "significant change" scan is completed, verify and document that the scans are performed by:

- qualified internal resources or qualified third parties
- a party whereby the scan tester is organizationally independent from the organization that made the significant change to the system components

Upon verification:

- detail how it was validated that the scan was performed by a qualified internal resource(s) or qualified external third party
- describe and document how the personnel who perform the scans demonstrated they are qualified to perform the scans.
- describe and document how organizational independence of the tester was observed to exist
- record the documentation with the scan reports and associated documentation

8.2.1.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections

PCI DSS Requirement 11.3.3 - Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

Policy: We correct exploitable vulnerabilities found during penetration testing and repeat testing to verify corrections have eliminated vulnerabilities identified.

Procedure: Upon identifying vulnerabilities during penetration testing the following steps are followed:

- document identified vulnerabilities
- correct vulnerabilities
- repeat penetration test to ensure identified vulnerabilities have been corrected and ensure that no new vulnerabilities have been introduced into the cardholder data environment as a result of the corrections
- document vulnerability resolution and final penetration testing results

8.2.1.4 Segmentation

PCI DSS Requirement 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 in-scope systems.

Policy: When segmentation is used to isolate the cardholder data environment (CDE) from other networks, penetration test procedures are defined and performed to identify and resolve vulnerabilities.

Procedure: Define and perform penetration test procedures that will:

- test all segmentation methodologies implemented within the CDE
- confirm that the segmentation methods are operational and effective
- ensure that segmentation methods isolate all out-of-scope systems from in-scope systems

8.2.2 Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files

PCI DSS Requirement 11.5 - Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

Policy: We require and have deployed a change-detection mechanism within the cardholder data environment to detect unauthorized modifications to critical system files, configuration files and content files and to alert personnel of unauthorized file changes.

A change-detection mechanism is to be deployed within the cardholder data environment and configured to:

- monitor the modification of critical system files, configuration files, and/or content files.
- alert personnel of unauthorized modification of critical system files, configuration files, and/or content files. These files include, but are not limited to the following:
    - System executables
    - Application executables
    - Configuration and parameter files
    - Centrally stored, historical or archived, log and audit files
    - Additional critical files determined by entity (i.e., through risk assessment or other means)
- perform critical file comparison at least weekly

Procedure: We will use automated software data collection and report analysis to identify and review all change-detection mechanisms deployed to ensure that they are configured to adhere to the guidelines above.

8.2.2.1 Implement a process to respond to any alerts generated by the change-detection solution

PCI DSS Requirement 11.5.1 - Implement a process to respond to any alerts generated by the change-detection solution.

Policy: We have implemented a process whereby the Cardholder Data Security Officer is notified of any alerts generated by the change-detection solution that are a result of changes that have been determined to be of established security concern and not false positives.

Procedure: All alerts produced by the change-detection system are immediately communicated to members of the Cardholder Data Security Team. Each alert is:

- logged
- responded to with an immediate investigation into the source of the change-detection alert
- verified to be of authentic security concern and deemed not to be a false positive

All alerts resulting from authentic security concerns are communicated to the Cardholder Data Security Officer. The Cardholder Data Security Officer and the Cardholder Data Security Team plan a response action to the alert, execute the response, and document the outcome of the response action plan.

9 Maintain an Information Security Policy

9.1 Information security policy for all personnel

PCI DSS Requirement 12 - Maintain a policy that addresses information security for all personnel

Policy: We have a security policy that addresses the security requirements and responsibilities for all personnel that use and/or maintain the cardholder data environment.

Procedure: When workforce personnel or system administrator personnel are assigned to perform duties that involve interaction with the cardholder data environment, they are informed of the organization security policy that:

- makes personnel aware of the sensitivity of the cardholder data
- informs personnel about their roles and duties involved with interacting with the cardholder data environment and cardholder data
- communicates to personnel their responsibility to protect cardholder data

Any revisions to the security policy are communicated to personnel as soon as they are put into effect.

9.1.1 Establish, publish, maintain, and disseminate a security policy

PCI DSS Requirement 12.1 - Establish, publish, maintain, and disseminate a security policy.

Policy: We have established an information security policy to details business and security practices required to protect cardholder data and the organization's information technology assets.
All personnel are notified of the policy upon initial employment with the organization and are made aware of any revisions to the policy on an ongoing basis.
Policy details communicate the sensitivity of the cardholder data and include references to clearly define roles and responsibilities that personnel have in protecting the data and ensuring compliance with the organization's security policies.

Procedure:

- Establish and maintain organization security policy detailing the security measures and practices used to protect:
  - the cardholder data environment system components.
  - cardholder data "at rest".
  - cardholder data in transmission.
- Publish the policy and revisions to the policy as soon as new security policies are put into effect.
- Disseminate the security policy and policy revisions using email, internal newsletters, training courses, and other methods deemed to be effective methods of communicating the policy to personnel.

9.1.2 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel

PCI DSS Requirement 12.4 - Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

Policy: All security policies clearly define information security responsibilities for all personnel.
It is the responsibility of the organization's business and security leadership, workforce personnel, and system component administrators to communicate their security requirements for the protection of cardholder data to the Cardholder Data Security Officer (CHDSO).

Procedure:

- The CHDSO shall coordinate resources to address the cardholder data security function required by the organization.

- The CHDSO will provide guidelines for securing cardholder data and system components within the cardholder data environment.
- The CHDSO will provide the supporting resources necessary to carry out the policy.
- All workforce personnel shall assume responsibility for complying with the organization's cardholder data security policies and shall be aware that violations may result in sanctions.
- Cardholder data system component responsibility owners shall ensure the security of their systems by coordinating and overseeing the successful execution of sound operating practices and policy compliance by those providing support.
- Independent audits of the cardholder data environment security program shall be performed on a periodic and recurring basis either by qualified personnel that are deemed to be independent or by qualified independent third parties.

9.1.3 Assign to an individual or team the following information security management responsibilities

PCI DSS Requirement 12.5 - Assign to an individual or team the following information security management responsibilities:

Policy: The organization has created a dedicated team to establish, implement and maintain all cardholder data and PCI DSS related security management responsibilities. This team will report to the Cardholder Data Security Officer.

Procedure: Each member of the team will be assigned specific responsibilities and duties pertaining to the protection of critical system components and cardholder data. Team members will be made clearly aware of their responsibilities and duties through specific policy implementation and training.

9.1.3.1 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations

PCI DSS Requirement 12.5.3 - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Policy: The Cardholder Data Security Officer is responsible for the establishing, documenting, distributing, and maintaining security incident response and escalation procedures.

Procedure: The Cardholder Data Security Officer will inform and educate the Cardholder Data Security Team on the policies and procedures designed to and facilitate the timely and effective handling of all security incidents responses.

9.1.4 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security

PCI DSS Requirement 12.6 - Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

Policy: We have implemented a formal security awareness program to inform and educate personnel about the important of cardholder data security.
Based on industry practices, the basis of our awareness program educates personnel on:

- applicable policies and laws associated with security awareness and the importance of compliance and the impact on cardholder data environment security.
- the relevant security terms such as vulnerabilities, threats, risk, asset (i.e. system component), and impact.
- discuss the system component assets and types of cardholder data to be protected and the reasons for safeguarding system components and cardholder data.
- state our organizations position and requirements for maintaining the confidentiality, integrity, and availability of cardholder data either when the cardholder data is stored or in transmission.
- describe various types of threats (malicious software including Trojans, viruses, and other types of malware) and vulnerabilities and how to recognize when and where security problems exist.
- address the rules of user behavior as well as describe the roles and responsibilities for complying with policies and procedures. Rules of behavior should include rules and policies associated with the use of email, web browsing, passwords, other technologies, and practices.
- roles and responsibilities of individuals either as workforce users, system component administrators, or security compliance administrators.
- continuing awareness and education can occur through the use of posters, letters, mailers, periodic training, internal email newsletters, and signage in common areas.
- all cardholder data environment users and system component administrators must sign an acknowledgement of the organization's security policy and acknowledge that they have participated in the awareness program and have been made aware of the organization's security policies and practices.

Procedure: Put security awareness program in place to educated personnel on the above policies as well as inform cardholder data environment users and system component administrators on new threats and security practices.

9.1.5 Maintain and implement policies and procedures to manager service providers with whom cardholder data is shared, or that could affect the security of cardholder data

PCI DSS Requirement 12.8 - 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:

Policy: We maintain and implement policies and procedures to manage service providers within whom cardholder data is shared, or that could affect the security of cardholder data in compliance with the.

Procedure: The following policies and procedures are applied to service providers:

- document the service provider's business entity information in a master list of service providers.
- ensure that any written agreements executed with my service provider to include an acknowledgement by the service provider that they are responsible for the security of cardholder data that service providers possess, store, process or transmit on behalf of our organization.
- perform proper due diligence is performed upon the service provider prior to engaging the service provider.
- monitor the service provider's PCI DSS compliance on an annual basis.
- document which PCI DSS requirements are managed by each service provider and which are managed by our organization.
-

9.1.5.1 Maintain a list of service providers

PCI DSS Requirement 12.8.1 - Maintain a list of service providers including a description of the service provided.

Policy: We maintain a list of all service providers used to store, process or transmit cardholder data.
Upon securing a business relationship with a service provider we:

- document the nature of the business relationship and the services provided by the service provider.
- document the service provider's business details in a master list of service providers that provider services that interact with, store or transmit cardholder data.
- update the service provider's information contained within the list when the business relationship changes or when the services provided to our organization by the service provider change in any way.

Procedure: We will use automated software data collection and report analysis to identify service providers that are linked to the network and cardholder data environment.

9.1.5.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer

PCI DSS Requirement 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 CDE.

Policy: We will identify all service provider organizations that process or maintain cardholder data. The following policy will be applied to service providers:

- such service provider businesses will sign Service Provider(s) Agreement(s) executed by the entity's name.
- written agreement maintained will includes an acknowledgement that the service provider(s) are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of our business, or to the extent that the service provider could impact the security of the our business' cardholder data environment
- we will establish the flow of cardholder data to all outside entities and identify how such information is transmitted, and the requirements for processing cardholder data at the service provider site.
- we will review all existing Service Provider Agreement and ensure that all such agreements are modified with Addendums or revised for compliance with PCI DSS Requirements and our security policies associated with securing, protecting, and safeguarding cardholder data.
- service provider entities must be required to report any instance of misuse or unauthorized disclosure of cardholder data. The termination of an agreement with the service provider must result in return or destruction of all cardholder data with the service provider entity.
- the service provider must train all members of their workforce that process or come into contact with cardholder data. This training must include awareness of the requirements of the PCI DSS Requirements and security standards as well as information about the service provider's security policies and procedures.
- we must have the right to audit the service provider in the event of violations related to its cardholder data.
- we must reserve the right to take "reasonable steps" including canceling the Service Provider Agreement with the entity without penalty.
- if the service provider intends to process or transmit the cardholder data outside the United States of America then we will be informed of specific details related to such processing or transmission and we reserve the right to not authorize any such flow of cardholder data.
- service providers are directly liable for failure to comply with PCI DSS Requirements.
- service providers must adhere to disclosure requirements as detailed in their Service Provider Agreement.

Procedure: We will use automated software data collection and report analysis to identify service providers and online backup providers that are linked to the network and cardholder data environment. We will use automated software data collection and report analysis to identify cardholder data on service located outside of a service provider's facilities that may be on physical servers located in a data center, or through a Cloud Service.

9.1.5.3 Ensure there is an established process for engaging service providers, including proper due diligence prior to engagement

PCI DSS Requirement 12.8.3 - Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

Policy: We have an established process used for engaging service providers that includes proper due diligence. After due diligence is performed, we complete a risk assessment prior to engaging a service provider entity.

Procedure: Upon identifying a service provider to address cardholder data processing requirement we:

- Request access to the service providers written information security program – we will ask questions that cover the following areas:

  - firewalls
  - intrusion detection systems and procedures
  - physical and logical access controls
  - monitoring system
  - incident response plan
  - personnel background checks
  - frequency of network vulnerability scanning and penetration testing
- **Require a Network Architecture Survey –**the service providers must complete questionnaire that requests specific information about its network architecture.
- **Investigate Service Provider Breach Response History** – we will ask the service provider to disclose past system breaches and their responses to the breaches, lessons learned, and about the breaches impact on cardholder data security and IT environment performance
- Validate the service provider's PCI DSS compliance
- **Conduct and onsite visit** –in the case there the service provider may access or store significant amounts of cardholder data, an on-site visit to the service provider's data processing center will be performed to validate PCI DSS compliance measures are in fact in place.
- **Review of the company's financial statements and business continuity plan** - for critical third parties the organization should review audited financial statements and the service provider's business continuity plan.
- Perform a Risk Management Assessment in compliance with PCI DSS guidance

9.1.5.4 Maintain a program to monitor service providers PCI DSS compliance status at least annually

PCI DSS Requirement 12.8.4 - Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

Policy:

- Within the Service Provider Agreement, service providers agree that their business entity will comply with the same PCI DSS Requirement that our organization must comply with to meet the requirements set forth by our organization's Card Payment Brand's Acquiring Bank with regards to the PCI DSS Requirements that our organization must meet.
- We perform a PCI DSS compliance review of all services provider entities that provide services to our organization whereby the services provided:
  - store cardholder data
  - transmit cardholder data
  - process cardholder data
  - perform scans and penetration testing services of our organization's cardholder data environment
- Enable our organization to comply with PCI DSS compliance policies, standards, and guidelines.
- The review of service provider compliance with PCI DSS Requirements occurs annually.
- Within the Service Provider Agreement executed with service provide entities, terms are clearly stated within the agreement whereby our organization has access to all PCI DSS Compliance testing documentation held by the service provider that is relevant to the services provided to our organization.

Procedure:

- Perform an annual review of the PCI DSS Requirements that must be met by our organization and the business entities of our service providers.
- Develop a PCI DSS compliance review specific to each service provider based on the services provided to our organization.
- Review each service provider's PCI DSS compliance audit reports, internal/external vulnerability scanning/rescanning reports, penetration testing reports, and any other reports that are relevant to the PCI DSS requirements compliance that must be met to comply with our organizations specific requirements.
- Review any change management documentation associated with significant changes to the system components operated by the service provider that are used to provide cardholder data environment services to our organization.
- Ensure that any deficiencies identified in the service provider's ability to comply with the PCI DSS Requirements are immediately brought to the Cardholder Data Security Officer attention for risk assessment and remediation.
- Document and record the service provider's PCI DSS Requirements compliance review performed by our organization and submit a Report of Service Provider Compliance to our organization's Cardholder Data Security Officer.

9.1.5.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity

PCI DSS Requirement 12.8.5 - Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

Policy: All PCI DSS requirements to be managed by our organization, and those managed by third-party service providers are clearly documented and maintained by the Cardholder Data Security Officer.
Procedure:

- We are to maintain written document that contains the specific details of the PCI DSS requirements that are managed by each service provider, and which are managed by our .organization (our company)
- The Cardholder Data Security Officer and the Cardholder Data Security Team are to reassess and reassign the PCI DSS requirements responsibility to be managed by our organization and third-party service providers as necessary before:
    - quarterly internal and external vulnerability scans, annual penetration tests.
    - scans and penetration tests that are to take place due to a significant change in the cardholder data environment.
- Revisions to the documented PCI DSS requirements to be managed by our organization or by a third party are to be made each time:
    - a new service provider is engaged to deliver services service provider whereby they are responsible for the security of cardholder data that their business operation possesses, stores, processes or transmits on behalf of our organization.
    - an existing service provider discontinues providing its services on behalf of our organization.

9.1.6 Implement an incident response plan. Be prepared to respond immediately to a system breach

PCI DSS Requirement 12.10 - Implement an incident response plan. Be prepared to respond immediately to a system breach.

Policy: We have implemented a system breach incident response plan. This plan has been:

- developed and disseminated by the Cardholder Data Security Officer to the Cardholder Data Security Team.
- read and understood by the Cardholder Data Security Team as acknowledged in writing by each team member.
- approved by our organization's management team with a clear understanding of their roles in working with the Chief Cardholder Data Security Officer and the Cardholder Data Security Team to minimize:
    - downtime of the business
    - unnecessary public media exposure
    - the creation of new legal liabilities

Procedure:

- The system breach incident response plan is to be developed and maintained by the Chief Cardholder Data Security Officer and the Cardholder Data Security Team.
- The system breach response plan is presented to the organization's business management team for review and approval.
- The business management team is required to review, amend, and approve the security breach response plan.
- During the review process, it would be sound business practice for the business management team to have the plan reviewed by the business organization's legal team and authorized, in writing, by the following teams and individuals:
    - legal team.
    - public relations team.
    - Chief Financial Officer, the Chief Information Officer, and the Chief Operations Officer.
    - and any other personnel that should be made aware of the security breach response plan and its associated responsibility and action assignments.
- The Cardholder Data Security Officer must maintain the plan, and, at a minimum, update the plan annually. Alternatively, the plan must be updated after significant changes to the business' operation (for example as a result of a merger or acquisition), or based on the addition of third-party service providers that have a significant impact on the cardholder data environment and our organization's security infrastructure, policies, and/or processes.
- The plan must be reviewed, updated, and approved by the business management team annually in compliance with any relevant risk management policies and practices.
-

9.1.6.1 Create the incident response plan to be implemented in the event of a breach

PCI DSS Requirement 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 back-up 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.

Policy: We have developed an incident response plan that is activated in the event of a system breach. Our incident response plan includes:

- Documented 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 back-up 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 whereby there cardholder data is processed by our organization.

Our incident response plan is tested annually.

Procedure: The incident response plan is disseminated:

- throughout the organization to ensure that all roles, responsibilities, and communication/contact strategies are clearly communicated to Cardholder Data Security Team Members and understood.
- to the business organization's officers so that they understand their roles and responsibilities.
- to service provider entities with which we are engaged so that they understand their roles and responsibilities

Upon execution of the plan in response to a system breach:

- all response actions are assigned to individual personnel, the Cardholder Data Security Officer, third-party service providers, or the organization's management team.
- all response procedures and actions undertaken by internal personnel are logged and the results are documented.
- all response procedures and actions undertaken by service providers are logged and the results are documented.
- notifications, discussions, and any other communications with cardholder brand issuers, acquiring banking partners, and third-party service providers are documented.
- a written confirmation that all data backed-up either on internal system components or on systems at service provider data centers has taken place in accordance with the processes defined within the incident response plan.