SpeedPro Greenville

Information Security Policy for PCI DSS Compliance

# About this Document

This document contains the SpeedPro Greenville information security policies. Detailed standards and processes that support this policy are described in associated standards and procedures documentation. This document is for internal use only and is not to be distributed.

# Table 1 - Revision History

| Version | Date | Author | Description of Change |
| --- | --- | --- | --- |
| 1.0 |  |  | Security Policy Created |
| 1.2 | November 2010 |  | Security Policy Updates |
| 2.0 | April 2011 | GWG | Update for PCI DSS v2.0 |
| 2.1 | March 2012 | TF | Update Doc references for NTP processes in Sect. 10 |
| 2.2 | March 2012 | ME | Formatting Updates |
| 3.0 | June 2014 | JJB | Update for PCI DSS v3.0 |
| 3.1 | July 2015 | JDB | Update for PCI DSS v3.1 and format standardization |
| 3.2 | July 2016 | MRS | Update for PCI DSS v3.2 |
| 3.2.1 | September 2018 | GWM | Update for PCI DSS v3.2.1 |
|  |  |  |  |

**Contents**

Information Security Policy for SAQ D Merchants 2

About this Document 3

Table 1 - Revision History 3

Introduction 8

Purpose / Scope 8

Security Policy Ownership and Responsibilities 9

Additional Process and Standards Documents Referenced by this Security Policy 10

Table 2 – Security Process and Standards Documents Referenced by Policy 10

Build and Maintain a Secure Network and Systems 11

1 Install and Maintain a Firewall Configuration to Protect Cardholder Data 11

1.1 Establish and Implement Firewall/Router Configuration Documentation 11

1.2 Restrict Connections between Untrusted Network Segments and the Cardholder Data Environment 12

1.3 Prohibit Direct Public Access between the Internet and any System Component in the Cardholder Data Environment 12

1.4 Personal Firewall Required on Mobile Computers 13

1.5 Security Policies and Operational Procedures Documentation 13

2 Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters 13

2.1 Change Vendor Supplied Defaults 13

2.2 System Hardening and Standard Configuration of Devices 13

2.3 Use Secure Protocols for Non-Console Access 14

2.4 System Inventory 14

2.5 Security Policies and Operational Procedures Documentation 14

2.6 Shared Hosting Providers 15

Protect Stored Cardholder Data 15

3 Protect Stored Data 15

3.1 Retention and Disposal of Sensitive Credit Card Account Data 15

3.2 Storage of Sensitive Credit Card Authentication Data 15

3.3 Mask Credit Card Numbers in Displays Wherever Possible 16

3.4 Store Sensitive Data in an Unreadable Format 16

3.5 Protection of Cryptographic Keys 16

3.6 Cryptographic Key Management Policies 17

3.7 Security Policies and Operational Procedures Documentation 18

4 Encrypt Transmission of Cardholder Data across Open, Public Networks 18

4.1 Transmission of Card Data over Public Networks 18

4.2 Transmission of Card Data via End User Messaging Technologies 18

4.3 Security Policies and Operational Procedures Documentation 19

Maintain a Vulnerability Management Program 19

5 Protect All Systems against Malware and Regularly Update Anti-virus Software or Programs 19

5.1 Deploy anti-virus software to protect systems 19

5.2 Ensure that all anti-virus mechanisms are current 19

5.3 Ensure that all anti-virus mechanisms are actively running 19

5.4 Security Policies and Operational Procedures Documentation 20

6 Develop and Maintain Secure Systems and Applications 20

6.1 Vulnerability risk ranking process 20

6.2 Regularly update systems and software 20

6.3 Secure Software Development 20

6.4 Change Control Procedures 21

6.5 Application Development 21

6.6 Protect Exposed Web Applications 22

6.7 Security Policies and Operational Procedures Documentation 22

Implement Strong Access Control Measures 22

7 Restrict Access to Cardholder Data by Business Need to Know 23

7.1 Restrict Access to Cardholder Data and Systems in Cardholder Data Environment 23

7.2 Access Control Systems 23

7.3 Security Policies and Operational Procedures Documentation 23

8 Identify and Authenticate Access to System Components 23

8.1 Require Unique User IDs 23

8.2 User Authentication Methods 24

8.3 Two-factor Authentication 24

8.4 Password Policy 24

8.5 Group or Shared Passwords 25

8.6 Other Authentication Mechanisms 25

8.7 Access to Database with Cardholder data 25

8.8 Security Policies and Operational Procedures Documentation 25

9 Restrict Physical Access to Cardholder Data 25

9.1 Limits and Monitor Physical Access to Systems 25

9.2 Employees and Visitor Identification 26

9.3 Physical Access Control 26

9.4 Identify and Authorize Visitors 26

9.5 Physically Secure All Media 27

9.6 Media Distribution 27

9.7 Media Storage and Accessibility 27

9.8 Media Destruction Policies and Procedures 27

9.9 Protection from Tampering and Substitution 27

9.10 Security Policies and Operational Procedures Documentation 28

Regularly Monitor and Test Networks 28

10 Track and Monitor All Access to Network Resources and Cardholder Data 28

10.1 Monitor System Components within the Cardholder Data Network 28

10.2 Generation of Audit Trails 28

10.3 Audit Trail Entries 29

10.4 Network and System Time Sync 29

10.5 Audit Trail Security 29

10.6 Log Review 29

10.7 Audit Trail History 30

10.8 Security Policies and Operational Procedures Documentation 30

11 Regularly Test Security Systems and Processes 30

11.1 Rogue Wireless Network Detection 30

11.2 Vulnerability Assessment Scans 31

11.3 Penetration Testing 31

11.4 Intrusion Detection/Prevention 32

11.5 Change Detection 32

11.6 Security Policies and Operational Procedures Documentation 32

Maintain an Information Security Policy 32

12 Maintain a Security Policy that Addresses Information Security for All Personnel 32

12.1 Publish, Distribute, and Update the Information Security Policy 32

12.2 Implement a Risk-Assessment Process 33

12.3 Critical Technology Usage Policies 33

12.4 Assign Information Security Responsibilities and Train Employees 33

12.5 Assign Information Security Management 34

12.6 Security Awareness Program 34

12.7 Background Checks 34

12.8 Policies for Sharing Data with Service Providers 34

12.9 Additional Requirements for Service Providers 35

12.10 Incident Response Plan Policies 35

Appendix A – Management Roles and Responsibilities 37

Assignment of Management Roles and Responsibilities for Security 37

Table A1 - Management Security Responsibilities 37

Appendix B – Agreement to ComplyAgreement to Comply with Information Security Policies 38

# Introduction

To safeguard SpeedPro Greenville‘sinformation technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects SpeedPro Greenville‘scommitment to comply with required standards governing the security of sensitive and confidential information.

SpeedPro Greenville can minimize inappropriate exposures of confidential or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses SpeedPro Greenville‘s information technology resources. It is the responsibility of employees, contractors, business partners, and agents of SpeedPro Greenville. Each should become familiar with this policy's provisions and the importance of adhering to it when using SpeedPro Greenville‘s computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the Owner.

# Purpose / Scope

The primary purpose of this security policy is to establish rules to ensure the protection of confidential or sensitive information and to ensure protection of SpeedPro Greenville‘s information technology resources. The policy assigns responsibility and provides guidelines to protect SpeedPro Greenville‘s systems and data against misuse or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to SpeedPro Greenville‘s data network. It may apply to users of information services operated or administered by SpeedPro Greenville (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with SpeedPro Greenville are subject to these same definitions and rules when they are using SpeedPro Greenville‘s information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks or data.

This security policy has been written to specifically address the security of data used by the Payment Card Industry.

Credit card data stored, processed or transmitted with SpeedPro Greenville’s Merchant ID must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Cardholder data within this document is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, and CVC2), Credit Card PIN, and any form of magnetic stripe data from the card (Track 1, Track 2).

# Security Policy Ownership and Responsibilities

The Owner is the assigned custodian of this Security Policy. It is the responsibility of the custodian of this security policy to publish and disseminate these policies to all relevant SpeedPro Greenville system users (including vendors, contractors, and business partners). In addition, the custodian(s) must see that the security policy addresses and complies with all standards SpeedPro Greenville is required to follow (such as the PCI DSS). This policy document will also be reviewed at least annually by the custodian(s) (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the custodian(s) listed above.

# Additional Process and Standards Documents Referenced by this Security Policy

This policy document defines the SpeedPro Greenville security policies relating to the protection of sensitive data and particularly credit card data. Details on SpeedPro Greenville standards and procedures in place to allow these policies to be followed are contained in other documents referenced by this policy. Table 2 lists other documents that accompany this security policy document, which help define SpeedPro Greenville data security best practices.

## Table 2 – Security Process and Standards Documents Referenced by Policy

Note: The document name references contained in this table and in footnotes throughout this security policy should be replaced with the company-specific standards document name.

| **Document Name** | **Location or Custodian** |
| --- | --- |
| Firewall and Router Configuration Standards | Custodian |
| System Hardening and Configuration Standards | Custodian |
| Full Data Retention and Storage Procedures | Custodian |
| Data Encryption and Key Management Procedures | Custodian |
| Vulnerability Discovery and Risk Ranking Process | Custodian |
| Software Development Life Cycle Process | Custodian |
| Physical Security Procedures | Custodian |
| NTP Configuration Procedures | Custodian |
| Operating Procedures | Custodian |
| Security Awareness Training Process | Custodian |
| Full Service Provider Compliance Validation Process | Custodian |
| Incident Response Plan | Custodian |
| Risk Assessment Process | Custodian |

# Build and Maintain a Secure Network and Systems

To protect sensitive or confidential data, it is critical to design and maintain a secure network infrastructure where this data can be stored, processed, or transmitted. The following polices cover the network infrastructure (hardware such as firewalls, routers, and switches) as well as requirements for the secure configuration of all system components (network hardware, servers, workstations, etc.).

## 1 Install and Maintain a Firewall Configuration to Protect Cardholder Data

Firewalls are devices that control computer traffic allowed between SpeedPro Greenville‘snetworks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity’s internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity’s trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet SpeedPro Greenville‘s specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in this requirement. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of requirement 1.

### 1.1 Establish and Implement Firewall/Router Configuration Documentation

SpeedPro Greenville will have documented Firewall/Router configuration standards[[1]](#footnote-1) that include the following:

* A formal process for approving and testing all network connections and changes to the firewall and router configurations. All changes must be tested to ensure the firewall/router rule set modifications were correctly implemented. (PCI DSS Requirement 1.1.1)
* A current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. (PCI DSS Requirement 1.1.2)
* A current diagram that shows all cardholder data flows across systems and networks. (PCI DSS Requirement 1.1.3)
* Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. (PCI DSS Requirement 1.1.4)
* Firewall configuration documentation must contain a description of groups, roles, and responsibilities for management of network components. (PCI DSS Requirement 1.1.5)
* Firewall configuration documentation must contain documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered insecure. (PCI DSS Requirement 1.1.6).
* A formal review of the firewall and router rule sets must be conducted at least every six months. They must be verified against the defined firewall/router configuration standards documentation. (PCI DSS Requirement 1.1.7).

### 1.2 Restrict Connections between Untrusted Network Segments and the Cardholder Data Environment

SpeedPro Greenville will restrict connections from untrusted network segments to system components within the cardholder data environment by doing the following:

Note: An “untrusted network” is any network that is external to the networks belonging to SpeedPro Greenville under review, or which are out of SpeedPro Greenville‘sability to control or manage (e.g., the Internet, connected vendor networks, public wireless networks). An “untrusted network may also include a lower security SpeedPro Greenville network that is used for normal business purposes but is not used for the storing, processing, or transmitting of sensitive data (e.g., corporate office networks).

* Firewall rules must limit all inbound and outbound traffic to/from the cardholder data network to only that which is necessary for business. (PCI DSS Requirement 1.2.1)
* Each router’s running configuration must be secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are power-cycled) must have the same secure configurations. (PCI DSS Requirement 1.2.2)
* When wireless networking is used, a firewall is required between any wireless network and the cardholder data environment. Firewall rules must prohibit insecure traffic and restrict traffic from the wireless segment to only that which is necessary for business. (PCI DSS Requirement 1.2.3)

### 1.3 Prohibit Direct Public Access between the Internet and any System Component in the Cardholder Data Environment

SpeedPro Greenville will prohibit direct public access between the Internet and any system component in the cardholder data environment by doing the following:

* Create a DMZ (using appropriate firewall configuration) to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. (PCI DSS Requirement 1.3.1)
* Limit all inbound traffic from the Internet to addresses within the DMZ. (PCI DSS Requirement 1.3.2)
* Direct network routes are prohibited (inbound or outbound) between the Internet and the segment of the cardholder data network where sensitive card data is persisted. (PCI DSS Requirement 1.3.3)
* Do not allow internal IP addresses (e.g., RFC 1918 address ranges) to pass from the Internet into the cardholder data network. (PCI DSS Requirement 1.3.3)
* Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (PCI DSS Requirement 1.3.4)
* Use a firewall that implements stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) (PCI DSS Requirement 1.3.5)
* All stored cardholder data must be kept within an internal network zone segmented from the DMZ and all other network segments with direct Internet access. (PCI DSS Requirement 1.3.6)
* Hide the structure of your internal network from the Internet using technologies such as NAT, PAT, RFC 1918 address space, proxy servers, etc. (PCI DSS Requirement 1.3.7.a)
* Disclosure of any private IP address, routing information, or internal structure of the cardholder data network to external entities requires approval from an authorized representative of SpeedPro Greenville. (PCI DSS Requirement 1.3.7.b)

### 1.4 Personal Firewall Required on Mobile Computers

* Personal firewalls must be installed and active on all mobile or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the cardholder data network. (PCI DSS Requirement 1.4)
* Personal firewall software is to be configured by SpeedPro Greenville to specific standards and configurations should not be alterable by mobile computer users. (PCI DSS Requirement 1.4)

### 1.5 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. (PCI DSS Requirement 1.5)

## 2 Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). SpeedPro Greenville‘sgeneral policy is to always change vendor-supplied defaults for system passwords and other security parameters before systems are installed in the secure network environment (cardholder data network).

Individuals with malicious intent (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

### 2.1 Change Vendor Supplied Defaults

* All vendor-supplied defaults must be changed on all system components before being used in the cardholder data network. (e.g., passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.). (PCI DSS Requirement 2.1.a, 2.2.d)
* All unnecessary default accounts must be removed or disabled before installing the device onto the network. (PCI DSS Requirement 2.1.b)
* If a wireless device is in use:
  + All default settings for wireless environments (equipment) connected to the cardholder data environment or transmitting cardholder data must be changed before enabling the wireless system for production use. (PCI DSS Requirement 2.1.1.a-e)
  + The encryption keys or passphrases must be changed anytime anyone with knowledge of the keys leaves the company or moves to a position that no longer requires knowledge of the keys. (PCI DSS Requirement 2.1.1.a)
  + Require that all wireless devices be configured or updated to support strong encryption technologies (i.e., WPA/WPA2) for both authentication to the network and transmission of data. (PCI DSS Requirement 2.1.1.d)

### 2.2 System Hardening and Standard Configuration of Devices

* Documented system configuration standards[[2]](#footnote-2) must:
* Be consistent with either SANS, ISO, NIST, CIS, or similar security industry standards and address PCI configuration requirements (e.g., password requirements, log settings, File Integrity Monitoring, Anti-virus software, etc.). (PCI DSS Requirement 2.2)
* Be developed that address all system components and address all known security vulnerabilities for systems used in the cardholder data network. (PCI DSS Requirement 2.2.a)
* Be updated as new vulnerabilities are identified. (See Section 6.1) (PCI DSS Requirement 2.2.b)
* Be applied when new systems used in the card network are configured and before systems are placed into production. (PCI DSS Requirement 2.2.c)
* Include only one primary function is implemented per server. If virtualization technologies are used, each virtual system or virtual component must have only one primary function. (PCI DSS Requirement 2.1.d, 2.2.1)
* Include unnecessary or insecure services, daemons, protocols are not enabled or are justified and documented as to the appropriate use of the service. (PCI DSS Requirement 2.2.d, 2.2.2)
* Include security parameter settings for all devices in the card network. (PCI DSS Requirement 2.2.d)
* Include additional security features implemented for insecure services, protocols or daemons. (PCI DSS Requirement 2.2.d, 2.2.3)
* Include all required functionality. These functions must support secure configuration, and only documented functionality may be present on systems in the card network. (PCI DSS Requirement 2.2.d, 2.2.4)
* Include the removal of all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers from system components in the cardholder network and document all enabled functions for each system. (PCI DSS Requirement 2.2.d, 2.2.5)

### 2.3 Use Secure Protocols for Non-Console Access

* Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components. (Use technologies such as SSH, VPN, or the latest secure versions of TLS for web-based management and other non-console administrative access.) (PCI DSS Requirement 2.3)

### 2.4 System Inventory

* Maintain a system inventory containing a list of hardware and software components, and a description of function/use for each item. (PCI DSS Requirement 2.4)

### 2.5 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI DSS Requirement 2.5)

### 2.6 Shared Hosting Providers

* Shared hosting providers must protect each entity’s hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*  (PCI DSS Requirement 2.6)

# Protect Stored Cardholder Data

Cardholder data (e.g., PAN and sensitive authentication data) must be protected when stored or in transit over public (or untrusted) networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. The following policies ensure proper encryption of stored data and data in transit over open, public networks.

## 3 Protect Stored Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the sensitive data is unreadable and unusable to that person.

Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

The following policies address the treatment of credit card data.

### 3.1 Retention and Disposal of Sensitive Credit Card Account Data

* Create SpeedPro Greenville data storage standards and procedures[[3]](#footnote-3). This document must detail how and where sensitive cardholder data is allowed to be stored within the organization (i.e., encrypted within a database, encrypted within backup media, encrypted within files on disk, within hardcopy documents, etc.). For each storage method and location, the document must define how long data is allowed to be kept (retention period) and contain a justification for its storage. (PCI DSS Requirement 3.1).
* SpeedPro Greenville data storage standards and procedures must document any legal, regulatory, or business requirements for cardholder data retention. (PCI DSS Requirement 3.1)
* All cardholder data older than the stated retention period(s) must be removed from storage locations (online, offline, printed, etc.). Document all data storage locations (transfer directories, copies of card data, backup directories, etc.) and see that they are covered under the data disposal requirements. (PCI DSS Requirement 3.1)
* An automatic or scheduled procedural process must be run or conducted at least quarterly to identify and remove cardholder data that exceeds retention requirements. (PCI DSS Requirement 3.1)

### 3.2 Storage of Sensitive Credit Card Authentication Data

* Never store sensitive cardholder data such as the authentication data (Track, CVC, and PIN) after an authorization event has taken place (even if encrypted). (PCI DSS Requirement 3.2).
* All sensitive authentication data must be deleted or rendered unrecoverable upon completion of the authorization process. (PCI DSS Requirement 3.2.c)
* If sensitive authentication data is received, it must be removed following the data destruction policies outlined in this document. (PCI DSS Requirement 3.2.d)
* Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) in any database, log file, debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.1).
* Never store the Card Validation Code (CVC) data (3 or 4 digit number located on the back or front of the credit card) in any database, log file, and debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.2).
* Never store the cardholders Personal Identification Number (PIN) data (includes actual PIN number or Encrypted PIN block obtained during a debit card transaction from the PIN Entry Device) in any database, log file, debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.3).

### 3.3 Mask Credit Card Numbers in Displays Wherever Possible

* Credit card PAN Data will be masked or truncated when displaying card numbers on any media. (PCI DSS Requirement 3.3)
* Only personnel with proper written approval may view the full PAN[[4]](#footnote-4).

### 3.4 Store Cardholder Data in an Unreadable Format

* All stored cardholder data (PAN at a minimum) must be rendered unreadable wherever it is persisted. This could be accomplished using a number of approaches. Examples include: use of strong cryptography with key management process and procedures, a one way hashing method, index tokens and pads, truncation methods, etc. (PCI DSS Requirement 3.4)
* Cardholder data (e.g., PAN) contained on any removable media (e.g., backup tapes) must be rendered unreadable (or remain unreadable) when media is removed from the system. (PCI DSS Requirement 3.4)
* If disk encryption is used to render sensitive data unreadable:
  + All logical access to encrypted file systems must be implemented via a mechanism that is separate from the native operating system authentication and access control mechanisms. Access to encrypted data cannot be granted based on an existing system authentication. (PCI DSS Requirement 3.4.1)
  + Decryption keys must be stored securely and protected with strong access controls. (PCI DSS Requirement 3.4.1)
  + When using disk encryption techniques, cardholder data on removable media must be encrypted wherever stored. Data must remain encrypted when the media is moved or be encrypted separately before being moved. (PCI DSS Requirement 3.4.1)

### 3.5 Protection of Cryptographic Keys

* A documented description of the cryptographic architecture used to protect cardholder data must be maintained. Description must include details of algorithms, protocols, and keys (including key usage, key strength, and expiry date) used to encrypt cardholder data. (PCI DSS Requirement 3.5.1)
* An inventory of Hardware Security Module(s) and/or Secure Cryptographic Devices must be maintained. (PCI DSS Requirement 3.5.1)
* Protect cryptographic keys used for encryption and decryption of cardholder data against disclosure and misuse. (PCI DSS Requirement 3.5)
* Access to encryption/decryption keys must be restricted to the fewest number of custodians necessary. (PCI DSS Requirement 3.5)
* Store data-encrypting key (DEK) in one or more of the following forms (PCIDSS 3.5.3):
  + Encrypted with a key-encrypting key (KEK) that is at least as strong and stored separately from the DEK.
  + Within a secure cryptographic device (i.e. – HSM or approved PTS approved POI device)
  + As key components or key shares in accordance with industry accepted methods.

### 3.6 Cryptographic Key Management Policies

Develop and document processes and procedures for encryption key management[[5]](#footnote-5). These procedures must include details for policies noted in section 3.5 above and the following items: (PCI DSS Requirement 3.6)

* If SpeedPro Greenvilleshares data encryption keys with customers, the customer must be provided with documentation regarding proper key management requirements (secure transmission, storage, and key update procedures) to meet SpeedPro Greenville policies and PC IDSS policies noted in 3.5 (PCI DSS Requirement 3.6a)
* Generate strong cryptographic keys (proper method, strength, and complexity). (PCI DSS Requirement 3.6.1)
* Distribution of all encryption keys utilized for encrypting cardholder data must be done in a secure manner. (PCI DSS Requirement 3.6.2)
* All encryption keys utilized for encrypting cardholder data must be securely stored. (PCI DSS Requirement 3.6.3)
* Encryption keys utilized to encrypt cardholder data must have a defined cryptoperiod and be changed at the end of the defined cryptoperiod. (PCI DSS Requirement 3.6.4)
* Old, invalid, compromised, or even suspected of compromise, data encryption keys must be retired or replaced then securely archived or destroyed. If asymmetric keys used for data encryption are registered with a certificate authority, then they must be revoked. (PCI DSS Requirement 3.6.5)
* Retired or replaced cryptographic keys must not be used for any encryption operations if they are retained. (PCI DSS Requirement 3.6.5)
* Manual clear-text key management procedures will require that the principles of split knowledge and dual control be applied to reconstruct a data encryption key. For example, a new key is generated; the new key is encrypted using a passphrase comprised of at least two individuals’ passphrases. These individuals do not share their part of the resulting passphrase. This ensures that no one individual can reconstruct the key alone, and no individual has knowledge of any part of the original key. (PCI DSS Requirement 3.6.6)
* Controls must be in place that will prevent the unauthorized substitution of encryption keys. (PCI DSS Requirement 3.6.7)
* Encryption key custodians must sign a form signifying they understand and accept their key-custodian responsibilities. (PCI DSS Requirement 3.6.8)

### 3.7 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for protecting stored cardholder data is documented, in use, and known to all affected parties. (PCI DSS Requirement 3.7)

## 4 Encrypt Transmission of Cardholder Data across Open, Public Networks

Cardholder data must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

### 4.1 Transmission of Card Data over Public Networks

* Strong encryption algorithms and protocols (i.e., TLS, IPSEC, SSH) must be used whenever cardholder data is transmitted or received over open, public networks. The following controls must be part of the SpeedPro Greenville data transmission policies: (PCI DSS Requirement 4.1.a)
* Only trusted keys or certificates will be accepted. (PCI DSS Requirement 4.1.b)
* The data transmission protocol must be implemented to use only secure protocol configurations, and must not support insecure versions or configurations (e.g., use the latest secure TLS and SSH versions only). (PCI DSS Requirement 4.1.c)
* The encryption strength is appropriate for the encryption methodology in use. (PCI DSS Requirement 4.1.d)
* For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (PCI DSS Requirement 4.1.e)
* If wireless networks transmitting cardholder data or connected to the cardholder data environment are in use, a documented standard must be created which ensures the use of strong encryption and industry best practices. (PCI DSS Requirement 4.1.1)

### 4.2 Transmission of Card Data via End User Messaging Technologies

* It is prohibited to transmit unencrypted cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (PCI DSS Requirement 4.2)

### 4.3 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for encrypting and transmissions of cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 4.3)

# Maintain a Vulnerability Management Program

System components within the cardholder data network must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g., anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained.

The following policies ensure system components are protected from malicious software and vulnerabilities that result from software bugs and improperly patched applications and operating systems.

## 5 Protect All Systems against Malware and Regularly Update Anti-virus Software or Programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters a sensitive network segment during many business approved activities, including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

### 5.1 Deploy anti-virus software to protect systems

* Anti-virus software must be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the cardholder network segment. (PCI DSS Requirement 5.1)
* Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (PCI DSS Requirement 5.1.1)
* For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti-virus software. (PCI DSS Requirement 5.1.2)

### 5.2 Ensure that all anti-virus mechanisms are current

* All anti-virus software and its associated definition files must be kept up-to-date at all times. (PCI DSS Requirement 5.2.a)
* All anti-virus software must be actively running, configured to perform automatic updates, and set to run periodic scans. (PCI DSS Requirement 5.2.b and c)
* Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year. (PCI DSS Requirement 5.2.d)

### 5.3 Ensure that all anti-virus mechanisms are actively running

* All anti-virus software installations and configurations must be actively running at all times. (PCI DSS Requirement 5.3.a)
* Anti-virus configurations do not allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time. (PCI DSS Requirement 5.3.b and c)

### 5.4 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. (PCI DSS Requirement 5.4)

## 6 Develop and Maintain Secure Systems and Applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

**Note:** Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.

For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

### 6.1 Vulnerability risk ranking process

* System administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (PCI DSS Requirement 6.1)
* When any vulnerability (or potential vulnerability) is found using the documented vulnerability discovery and risk ranking process[[6]](#footnote-6), it must be evaluated and assigned a ranking based on the risk level. At a minimum, the highest risk vulnerabilities should be assigned a “High” risk ranking. (PCI DSS Requirement 6.1)

### 6.2 Regularly update systems and software

* All system components and software must have the latest vendor-supplied security patches installed. (PCI DSS Requirement 6.2.a)
* All critical system and software patches must be installed within 30 days of vendor release. (PCI DSS Requirement 6.2.b)

### 6.3 Secure Software Development

* Software developed by SpeedPro Greenville is used to store, process, or transmit sensitive card data. The following policies ensure that this software is developed and tested in a secure manner:
  + Develop software applications based on industry best practices and in accordance with the PCI DSS. Incorporate information security throughout the software development life cycle (SDLC). These SDLC processes and procedures[[7]](#footnote-7) must be documented and followed. (PCI DSS Requirement 6.3.a)
  + Information security must be included throughout the software development lifecycle. (PCI DSS Requirement 6.3.b)
  + Software applications must be developed in accordance with all PCI DSS requirements. (PCI DSS Requirement 6.3.c)
  + All custom or default application accounts, user IDs, and passwords used for testing or development are to be removed before software is moved into the production cardholder data environment or delivered to customers. (PCI DSS Requirement 6.3.1)
  + All custom code must be reviewed prior to release in the production environment or to customers. (PCI DSS Requirement 6.3.2)
  + Code reviews must be conducted by an individual other than the original code author who is knowledgeable in code review techniques and secure coding practices. (PCI DSS Requirement 6.3.2)
  + Code is developed in accordance with secure coding guidelines defined as per PCI DSS 6.5. (PCI DSS Requirement 6.3.2)
  + Corrections are implemented prior to release if necessary. (PCI DSS Requirement 6.3.2)
  + Code review results must be reviewed and approved by management prior to release. (PCI DSS Requirement 6.3.2)

### 6.4 Change Control Procedures

* Separate the development/test environment from the production environment, and enforce the separation with access controls. (PCI DSS Requirement 6.4.1)
* Separation of duties must be in place between personnel working in the development/test environment and those working in production environments. (PCI DSS Requirement 6.4.2)
* Production data (live credit card PAN data) is not to be used for testing or development purposes. (PCI DSS Requirement 6.4.3)
* All test data and test accounts are to be removed before the application becomes active. (PCI DSS Requirement 6.4.4)
* Change control tracking procedures detailed in the SDLC documentation must capture all changes to system components in the cardholder data network. This includes implementations of security patches and software modifications. (PCI DSS Requirement 6.4.5)
* Change control documentation must include impact documentation. (PCI DSS Requirement 6.4.5.1)
* Change control documentation must record sign-off by authorized parties. (PCI DSS Requirement 6.4.5.2)
* Change control documentation must show that functionality testing has verified the change does not adversely affect the security of the system and all updates are tested for compliance with PCI DSS Requirement 6.5 prior to deployment to production. (PCI DSS Requirement 6.4.5.3)
* Change control documentation must contain back-out procedures that can be used to return systems to a state before the change was made. (PCI DSS Requirement 6.4.5.4)
* Change control procedures must require a review to ensure all relevant PCI DSS requirements have been implemented on all systems affected by a significant change. (PCI DSS Requirement 6.4.6)

### 6.5 Application Development

* All applications developed for internal or external exposure hosted within the cardholder data environment (including all web-based administrative interfaces) must be developed in accordance with industry standard secure coding guidelines (such as the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.). (PCI DSS Requirement 6.5)
* All developers must be trained in secure coding techniques, including how to avoid common coding vulnerabilities, and understand how sensitive data is handled in memory. (PCI DSS Requirement 6.5)
* SDLC documentation must contain processes that ensure that applications are developed so they will not be vulnerable to common vulnerabilities, such as:
  + Injection flaws. (PCI DSS Requirement 6.5.1)
  + Buffer overflows. (PCI DSS Requirement 6.5.2)
  + Insecure cryptographic storage. (PCI DSS Requirement 6.5.3)
  + Insecure communications. (PCI DSS Requirement 6.5.4)
  + Improper error handling. (PCI DSS Requirement 6.5.5)
  + All “high risk” vulnerabilities identified in PCI DSS Requirement 6.1. (PCI DSS Requirement 6.5.6)
  + Specifically for web applications and application interfaces:
    - Cross-site scripting (XSS). (PCI DSS Requirement 6.5.7)
    - Improper access control. (PCI DSS Requirement 6.5.8)
    - Cross-site Request Forgery (CSRF). (PCI DSS Requirement 6.5.9)
    - Broken Authentication and Session Management (PCI DSS Requirement 6.5.10)
* As industry best practices for secure development and vulnerability management are updated, SpeedPro Greenville will have a process in place to modify secure coding and vulnerability management practices to stay in sync with the most recent developments. Procedures related to PCI DSS 6.5.1-6.5.10 will be modified to match industry best practices. (PCI DSS Requirement 6.5)

### 6.6 Protect Exposed Web Applications

Protect exposed web applications by implementing at least one of the following:

* Public-facing web applications must be reviewed (using either manual or automated vulnerability security assessment tools or methods) as follows: (PCI DSS Requirement 6.6)
  + At least annually.
  + After any changes.
  + By an organization that specializes in application security (can be a separate internal company team, independent of the development team that has been trained appropriately).
  + All vulnerabilities in PCI DSS Requirement 6.5 are included.
  + All vulnerabilities must be corrected before being made live.
  + The application is re-evaluated after corrections have been made.
* 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, which continually checks all traffic. The solution must meet the following requirements:(PCI DSS Requirement 6.6)
  + Is situated in front of public-facing web applications.
  + Is actively running and updated as applicable.
  + Is generating audit logs.
  + Is configured to either block web-based attacks, or generate an alert.

### 6.7 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for developing and maintaining secure system and applications are documented, in use, and known to all affected parties. (PCI DSS Requirement 6.7)

# Implement Strong Access Control Measures

Access to system components and software within the cardholder data network must be controlled and restricted to those with a business need for that access. This is achieved using active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a “need to know”.

## 7 Restrict Access to Cardholder Data by Business Need to Know

Systems and processes must be in place to limit access to critical data and systems based on an individual’s need to know and according to job responsibilities.

Need to know is when access rights are granted to the least amount of data and privileges needed to perform a job.

### 7.1 Restrict Access to Cardholder Data and Systems in Cardholder Data Environment

* Access to cardholder data and system components must be restricted to only those individuals whose job requires such access. (PCI DSS Requirement 7.1)
* Define access needs for each role, including: (PCI DSS Requirement 7.1.1)
  + System components and data resources that each role needs to access for their job function.
  + Level of privilege required for accessing resources (for example, User, Administrator, etc.).
* Restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require the privileged access. (PCI DSS Requirement 7.1.2)
* Access assigned to individual personnel is based on their job classification and function. (PCI DSS Requirement 7.1.3)
* An authorization form specifying all required access privileges is required and must be generated and signed by management approving the access. (PCI DSS Requirement 7.1.4)

### 7.2 Access Control Systems

* Access control systems for systems components must restrict access based on a user’s need to know. (PCI DSS Requirement 7.2)
* Access controls are required on all system components of the cardholder data environment and must be implemented via an automated access control system. (PCI DSS Requirements 7.2.1)
* Access controls are required to enforce privileges assigned to individuals based on job classification and function. (PCI DSS Requirements 7.2.2)
* Access control systems must also be set to a default “deny-all” setting. (PCI DSS Requirements 7.2.3)

### 7.3 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 7.3)

## 8 Identify and Authenticate Access to System Components

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

### 8.1 Require Unique User IDs

* Unique IDs will be used for all users that access system components in the cardholder data environment. (PCI DSS Requirement 8.1)
* Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. (PCI DSS Requirement 8.1.2)
* Immediately revoke access for any terminated users. (PCI DSS Requirement 8.1.3)
* Remove/disable inactive user accounts at least every 90 days. (PCI DSS Requirement 8.1.4)
* Manage IDs used by vendors to access, support, or maintain system components via remote access, ensuring that they are only enabled for the time period needed, disabled when not in use and they are monitored by SpeedPro Greenville employees during use. (PCI DSS Requirement 8.1.5)
* Limit repeated access attempts by locking out the user ID after no more than six attempts. (PCI DSS Requirement 8.1.6)
* Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. (PCI DSS Requirement 8.1.7)
* If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (PCI DSS Requirement 8.1.8)

### 8.2 User Authentication Methods

* In addition to assigning a unique user ID, access to systems in the card network requires the use of at least one of the following: (PCI DSS Requirement 8.2)
  + Something you know, like a password or passphrase
  + Something you have, like a token device or smart card
  + Something you are, like a Biometric
* Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. (PCI DSS Requirement 8.2.1)
* Verify user identity before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys.) (PCI DSS Requirement 8.2.2)
* Passwords or phrases must meet the following: (PCI DSS Requirement 8.2.3)
  + Require a minimum length of at least seven characters
  + Contain both numeric and alphabetic characters
* Change user passwords/passphrases at least every 90 days. (PCI DSS Requirement 8.2.4)
* Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/phrases they have used. (PCI DSS Requirement 8.2.5)
* Set all first time use and reset passwords to a unique value for each user and require immediate change after first use. (PCI DSS Requirement 8.2.6)

### 8.3 Multi-factor Authentication

* Incorporate multi-factor authentication for all non-console administrative access to the cardholder data environment (CDE). Multi-factor authentication is also required for all remote access originating from outside the CDE by personnel, including users and administrators and all third parties, including vendor access for support or maintenance. (PCI DSS Requirement 8.3)

### 8.4 Password Policy

* Document and communicate authentication procedures and policies to all users including: (PCI DSS Requirement 8.4)
  + Guidance on selecting strong authentication credentials.
  + Guidance for how users should protect their authentication credentials.
  + Instructions not to reuse previously used passwords.
  + Instructions to change passwords if there is any suspicion the password could be compromised.

### 8.5 Group or Shared Accounts and Passwords

* Do not use group, shared, or generic accounts or passwords or other authentication methods as follows: (PCI DSS Requirement 8.5.)
  + 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.

### 8.6 Other Authentication Mechanisms

* 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: (PCI DSS Requirement 8.6)
  + Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
  + Physical or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

### 8.7 Access to Database with Cardholder data

* All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: (PCI DSS Requirement 8.7)
  + All user access to, user queries of, and user actions on databases are through programmatic methods.
  + Only database administrators have the ability to directly access or query databases.
  + Application IDs for database applications can only be used by the applications and not by individual users or other non-application processes.

### 8.8 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. (PCI DSS Requirement 8.8)

## 9 Restrict Physical Access to Cardholder Data

Any physical access to data or systems that house cardholder data provide the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

**Note:** For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

### 9.1 Limits and Monitor Physical Access to Systems

* Physical security controls must exist for each computer room, data center, and any other physical areas that contain systems in the cardholder data environment. Use security systems such as badge readers, lock and key, etc. to control access to these areas. (PCI DSS Requirement 9.1)
* Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. These mechanisms must be protected from tampering or being disabled, and they must be reviewed and correlated with other entries. Store access data for at least three months. (PCI DSS Requirement 9.1.1)
* Restrict access to network jacks by implementing physical and logical controls. (PCI DSS Requirement 9.1.2)
* Restrict physical access to wireless access points, gateways, network hardware and handheld devices. (PCI DSS Requirement 9.1.3)

### 9.2 Employees and Visitor Identification

* Develop procedures[[8]](#footnote-8) that allow easy distinction between employees and visitors in areas where cardholder data is accessible. These processes must include the following: (PCI DSS Requirement 9.2)
  + Process for identifying new onsite personnel or visitors (for example assigning badges).
  + Process for making changes to access requirements.
  + Process for revoking or terminating onsite personnel and expired visitor identification (such as ID badges).
  + All administrative access to the badge system must be limited to only authorized personnel.

### 9.3 Physical Access Control

* Control physical access for onsite personnel to the sensitive areas as follows: (PCI DSS Requirement 9.3)
  + Access must be authorized and based on individual job function.
  + Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

### 9.4 Identify and Authorize Visitors

* SpeedPro Greenville will define and implement procedures7 required to identify and authorize visitors to include the following: (PCI DSS Requirement 9.4)
  + Visitors are authorized before entering and escorted at all times within areas where cardholder data is processed or maintained. (PCI DSS Requirement 9.4.1)
  + Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. (PCI DSS Requirement 9.4.2.a)
  + Visitor badges or other identification must expire at the end of the authorized access time period. (PCI DSS Requirement 9.4.2.b)
  + Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. (PCI DSS Requirement 9.4.3)
  + A visitor log with the visitors name, the firm represented, and the onsite personnel authorizing physical access is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. The log will be kept for a minimum of three months, unless otherwise restricted by law. (PCI DSS Requirement 9.4.4)

### 9.5 Physically Secure All Media

* SpeedPro Greenville will define specific procedures[[9]](#footnote-9) to physically secure all media, including but not limited to computers, removable electronic media, paper receipts, paper reports and faxes. (PCI DSS Requirement 9.5)
* Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location’s security at least annually. (PCI DSS Requirement 9.5.1)

### 9.6 Media Distribution

* Maintain strict control over the internal or external distribution of any kind of media, including the following: (PCI DSS Requirement 9.6)
  + Classify media so the sensitivity of the data can be determined.
  + Send the media by secured courier or other delivery method that can be accurately tracked. Logs must show management approval, and tracking information. Retain media transfer logs.
  + Ensure management approves all media that is moved from a secured area, including when media is distributed to individuals.

### 9.7 Media Storage and Accessibility

* Maintain strict control over the storage and accessibility of media. (PCI DSS Requirement 9.7)
* Properly maintain inventory logs of all media and conduct media inventories at least annually. (PCI DSS Requirement 9.7)

### 9.8 Media Destruction Policies and Procedures

* Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. (PCI DSS Requirement 9.8)
* SpeedPro Greenville must define and document specific procedures[[10]](#footnote-10) that will be used to destroy, beyond reconstruction, any hard copy materials containing cardholder data. Technologies such as shredding, incineration, pulping, etc. must be used to destroy media. (PCI DSS Requirement 9.8.1)
* Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or the media must be physically destroyed. (PCI DSS Requirement 9.8.2)
* If applicable, all containers used to store media containing cardholder data to be destroyed must be locked and in a secure area at all times. Such containers are only to be given to authorized personnel or third parties for the purpose of destruction. (PCI DSS Requirement 9.8.1.b)

### 9.9 Protection from Tampering and Substitution

* Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. (PCI DSS Requirement 9.9)
* Maintain an up to date list of devices including the following: (PCI DSS Requirement 9.9.1)
  + Make and model of the device.
  + Location of the device.
  + Device serial number or other method of unique identification.
* Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been replaced with a fraudulent device). (PCI DSS Requirement 9.9.2)
* Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI DSS Requirement 9.9.3)
  + Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
  + Do not install, replace, or return devices without verification.
  + Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
  + Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

### 9.10 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 9.10)

# Regularly Monitor and Test Networks

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing.

## 10 Track and Monitor All Access to Network Resources and Cardholder Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs. Detailed monitoring procedures should be developed and documented to meet the following policies.

### 10.1 Monitor System Components within the Cardholder Data Network

* Enable audit trails on all system components within the cardholder data network to link all access to system components to each individual user. (e.g., server event logs, web server logs, firewall logs, payment application logs, etc.). (PCI DSS Requirement 10.1)

### 10.2 Generation of Audit Trails

* Implement automated audit trails for all system components to capture the following events: (PCI DSS Requirement 10.2)
  + All individual access to cardholder data.
  + All actions taken by any individual with root or administrative privileges.
  + All access to audit trails.
  + Invalid logical access attempts.
  + 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.
  + Initialization, stopping, or pausing the audit logs.
  + Creation and deletion of system level objects.

### 10.3 Audit Trail Entries

* Record at least the following audit trail entries for all system components for each event: (PCI DSS Requirement 10.3)
  + User Identification
  + Type of event
  + Date and Time
  + Origination of event
  + Identity or name of affected data, system component, or resource

### 10.4 Network and System Time Sync

* Define and document the process[[11]](#footnote-11) for obtaining and distributing a time signal (system time) to all system components within the cardholder data network. (PCI DSS Requirement 10.4)
* Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time: (PCI DSS Requirement 10.4)
  + A central timeserver is designated, and if there are multiple servers, the servers are configured to peer with each other to keep accurate time.
  + All other components in the CDE receive time only from the designated central timeserver.
  + Critical systems have the correct and consistent time.
  + Time data is protected through access to time data restricted to only personnel with a business need.
  + All time settings on critical systems are logged, monitored, and reviewed.
  + Time settings are received from industry-accepted sources.

### 10.5 Audit Trail Security

* Secure audit trails so they cannot be altered as follows: (PCI DSS Requirement 10.5)
  + Limit viewing of audit trails to those with a job-related need.
  + Protect audit trail files from unauthorized modifications.
  + Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
  + Write logs for external-facing technologies onto a secure, centralized log server or media device.
  + Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.

### 10.6 Log Review

* Review logs and security events for all system components to identify anomalies or suspicious activity by performing the following: (PCI DSS Requirement 10.6)
  + Review the following at least daily:
    - All security events.
    - Logs of all system components that store, process, or transmit cardholder data, or that could affect the security of cardholder data.
    - Logs of all critical system components.
    - Logs of all servers and system components that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.).
* 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[[12]](#footnote-12).
* Immediately follow up on exceptions and anomalies identified during the review process. (PCI DSS Requirement 10.6.3.a)

### 10.7 Audit Trail History

* Retain audit trail history for at least one year with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup). (PCI DSS Requirement 10.7)

### 10.8 Internal Auditing of Security Controls

* Automated or manual processes must be in place for timely detection and reporting of failures of critical security control systems (firewalls, IDS/IPS, FIM, anti-virus, access controls, segmentation controls, etc.). (PCI DSS Requirement 10.8)
* Response to failures in critical security controls must be performed in a timely manner. Response to failures must include restoring proper functionality, documenting the duration of the failure, documenting the cause of the failure, performing a risk assessment, implementing controls to prevent reoccurrence of the failure, and resuming monitoring of the security control. (PCI DSS Requirement 10.8.1)

### 10.9 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 10.9)

## 11 Regularly Test Security Systems and Processes

Vulnerabilities are continually being discovered in current, and introduced by new software. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures[[13]](#footnote-13) should be developed and documented to meet the following policies.

### 11.1 Rogue Wireless Network Detection

* SpeedPro Greenville will have a documented process[[14]](#footnote-14) that will be used at least quarterly to detect unauthorized wireless networks/devices within the card-processing environment. (PCI DSS Requirement 11.1 and 11.1.2)
* The defined process will address the detection and identification of multiple types of wireless devices such as WLAN cards inserted into system components, portable wireless devices connected to system components, and wireless devices connected to a network port or network device. (PCI DSS Requirement 11.1)
* Any automated wireless monitoring solution must generate alerts if rogue devices are detected.
* Process documentation must define a response procedure if rogue devices are found.
* SpeedPro Greenville will maintain an inventory of all authorized wireless access points including a documented business justification. (PCI DSS Requirement 11.1.1)
* SpeedPro Greenville will define incident response procedures (see PCI DSS Requirement 12.10) in the event an unauthorized wireless access point is detected (PCI DSS Requirement 11.1.2)

### 11.2 Vulnerability Assessment Scans

* Internal and external vulnerability assessment scans must be performed at least quarterly and after any significant change in the cardholder data network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). (PCI DSS Requirement 11.2)
* Internal vulnerability scans must: (PCI DSS Requirement 11.2.1.a-c)
  + Be performed quarterly.
  + Performed by a qualified internal resource with organizational independence or a qualified third party.
  + Have a process to include a rescan until all “high-risk” vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.
* External vulnerability scans must (PCI DSS Requirement 11.2.2.a-c)
  + Be performed quarterly.
  + Be performed by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) with rescans until passing scans are achieved.
  + Contain no vulnerabilities that are scored 4.0 or higher by the CVSS.
  + Run on all external IP addresses that could be used to gain access to the cardholder data environment. (PCI DSS Requirement 11.2)
* Ensure that results of each quarter’s internal and external vulnerability assessments are to be documented and retained for review. (PCI DSS Requirement 11.2.3)

### 11.3 Penetration Testing

* Implement a methodology for penetration testing that includes the following: (PCI DSS Requirement 11.3)
  + Is based on industry-accepted penetration testing approaches. (for example, NIST SP 800-115)
  + Includes coverage for the entire CDE perimeter and critical systems.
  + Includes testing from both inside and outside the network.
  + Includes testing to validate all segmentation and scope reducing controls.
  + Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
  + Defines network-layer penetration tests to include components that support network functions as well as operating systems.
  + Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
  + Specifies retention of penetration testing results and remediation activity results for at least one year.
* Internal and external penetration tests are to be performed as per the defined methodology, at least annually and after any significant change in the environment (e.g., an operating system upgrade, a sub-network added to the environment, or a web server added to the environment, etc.). All external IP addresses that could be used to gain access to the cardholder data environment must be tested. (PCI DSS Requirement 11.3.1 and 11.3.2)
* Penetration testing is to be performed by a qualified internal resource or third party. If an internal resource is used, the personnel conducting the test must be independent from personnel that work within the cardholder environment. (PCI DSS Requirement 11.3)
* Noted exploitable vulnerabilities found are corrected and testing is repeated to confirm the correction. (PCI DSS Requirement 11.3.3)
* If segmentation is used to isolate the CDE from other networks, perform segmentation 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. (PCI DSS Requirement 11.3.4)

### 11.4 Intrusion Detection/Prevention

* All traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder environment must be monitored by the use of an Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS). (PCI DSS Requirement 11.4.a)
* The IDS/IPS system(s) must be configured to alert personnel of suspected compromises. (PCI DSS Requirement 11.4.b)
* All IDS/IPS system(s) must be kept up-to-date with the latest available attack signatures. (PCI DSS Requirement 11.4.c)

### 11.5 Change Detection

* 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. (PCI DSS Requirement 11.5)

### 11.6 Security Policies and Operational Procedures Documentation

* Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 11.6)

# Maintain an Information Security Policy

Without strong security policies and procedures, many of the layers of security controls become ineffective at preventing data breach. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the SpeedPro Greenville security policies described in this document.

## 12 Maintain a Security Policy that Addresses Information Security for All Personnel

A strong security policy sets the security tone for SpeedPro Greenville and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

**Note:** “Employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.

### 12.1 Publish, Distribute, and Update the Information Security Policy

* SpeedPro Greenville requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI DSS Requirement 12.1)
* The SpeedPro Greenville information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (PCI DSS Requirement 12.1.1)

### 12.2 Implement a Risk-Assessment Process

* SpeedPro Greenville must define and document a risk assessment process[[15]](#footnote-15) which:
  + Is performed annually and upon significant change to the environment
  + Identifies critical assets, threats, and vulnerabilities
  + Results in a formal risk assessment.(PCI DSS Requirement 12.2)

### 12.3 Critical Technology Usage Policies

* SpeedPro Greenville must develop usage policies for all critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage), and define proper use of these technologies. (PCI DSS Requirement 12.3)
* Explicit management approval is required prior to using the technologies. (PCI DSS Requirement 12.3.1)
* Any use of the technology must be authenticated with a user ID and password or other authentication item (for example, token). (PCI DSS Requirement 12.3.2)
* A list must be maintained of all such devices in use and contain the personnel authorized to use them[[16]](#footnote-16). (PCI DSS Requirement 12.3.3)
* A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices). (PCI DSS Requirement 12.3.4)
* Acceptable uses for the technology must be defined and documented[[17]](#footnote-17). (PCI DSS Requirement 12.3.5)
* Acceptable network locations for the technologies must be defined and documented. (PCI DSS Requirement 12.3.6)
* A list of company-approved products must be kept. (PCI DSS Requirement 12.3.7)
* Remote-access technologies in use must automatically disconnect sessions after a specific period of inactivity. (PCI DSS Requirement 12.3.8)
* Only activate remote-access technologies for vendors and business partners when needed and immediately deactivate remote-access sessions after use. (PCI DSS Requirement 12.3.9)
* Copying, moving, or storing cardholder data on local hard drives, and removable electronic media when accessing such data via remote-access technologies is prohibited unless explicitly authorized for a defined business need, and the cardholder data is protected in accordance with all applicable PCI DSS requirements. (PCI DSS Requirement 12.3.10)

### 12.4 Assign Information Security Responsibilities

* Executive management will assign overall accountability for maintaining PCI DSS compliance to a group or individual as outlined in the SpeedPro Greenville PCI DSS compliance charter. Communication between executive management and those responsible for overseeing compliance efforts will follow requirements outlined in the charter. (PCI DSS Requirement 12.4.1)
* The SpeedPro Greenville‘s information security policy and procedures apply to all employees (full, part-time, or work study employees), contractors, and individuals providing services for SpeedPro Greenville and could affect security of cardholder information. (PCI DSS Requirement 12.4)

### 12.5 Assign Information Security Management

* The overall responsibility of information security at *SpeedPro Greenville* falls under the office of <Role or Department>. (PCI DSS Requirement 12.5)
* Specifically the following responsibilities must be assigned: (see form in Appendix A)
  + Establishing, documenting and distributing the SpeedPro Greenville information security policies and procedures. (PCI DSS Requirement 12.5.1)
  + Responsibility to monitor, analyze, and distribute security alerts and information. (PCI DSS Requirement 12.5.2)
  + Establish detailed documentation of security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific role, position, or team. (PCI DSS Requirement 12.5.3)
  + Administration of user accounts in the cardholder data network. (PCI DSS Requirement 12.5.4)
  + Monitoring and controling all access to data. (PCI DSS Requirement 12.5.5)

### 12.6 Security Awareness Program

* A formal security awareness program[[18]](#footnote-18) must exist and participation is required for all employees working within the cardholder data environment. (PCI DSS Requirement 12.6.a)
* Employees working in the cardholder data environment must be educated upon hire and at least annually regarding their data security responsibilities. (PCI DSS Requirement 12.6.b)
* Security awareness training programs must employ the use of multiple methods of communicating awareness and educating employees (e.g., posters, letters, memos, web, meetings, etc.). (PCI DSS Requirement 12.6.1.a)
* Employees must acknowledge in writing, at least annually, that they have read and understood the SpeedPro Greenville security policies and procedures. (PCI DSS Requirement 12.6.2)

### 12.7 Background Checks

* Background checks are to be conducted, within the constraints of local laws, on employees, prior to hire, who will have access to cardholder data or the cardholder data environment. (PCI DSS Requirement 12.7)

### 12.8 Policies for Sharing Data with Service Providers

* In order to conform to industry best practices, it is required that due diligence be performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on SpeedPro Greenville’s behalf. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy.
* SpeedPro Greenville shall maintain a documented list[[19]](#footnote-19) of all applicable service providers in use. (PCI DSS Requirement 12.8.1)
* A written agreement with all applicable service providers is required and must include an acknowledgement of the service providers’ responsibility for securing all cardholder data they receive from or on behalf of SpeedPro Greenville, or to the extent that they could affect the security of a cardholder data environment (PCI DSS Requirement 12.8.2). In addition, the service provider must agree to provide compliance validation evidence on an annual basis. (PCI DSS Requirement 12.8.4). Prior to engaging with an applicable service provider, a thorough due diligence process[[20]](#footnote-20) should be followed. (PCI DSS Requirement 12.8.3)
* SpeedPro Greenville shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance. (PCI DSS Requirement 12.8.4)
* SpeedPro Greenville shall maintain a list[[21]](#footnote-21) of which PCI DSS requirements are managed by each service provider, and which are managed by SpeedPro Greenville. (PCI DSS Requirement 12.8.5)

### 12.9 Additional Requirements for Service Providers

* Service providers must acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. (PCI DSS Requirement 12.9)

### 12.10 Incident Response Plan Policies

Incidents or suspected incidents regarding the security of the cardholder data network or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan (IRP) must be developed and followed in the event of a breach or suspected breach. The following policies specifically address the SpeedPro Greenville IRP[[22]](#footnote-22):

* SpeedPro Greenville must maintain a documented IRP and be prepared to respond immediately to a system breach. (PCI DSS Requirement 12.10)
* The IRP must clearly define roles and responsibilities for response team members. (PCI DSS Requirement 12.10.1)
* The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands. (PCI DSS Requirement 12.10.1)
* The IRP must define specific incident response procedures to be followed. (PCI DSS Requirement 12.10.1)
* The IRP must document business recovery and continuity procedures. (PCI DSS Requirement 12.10.1)
* The IRP must detail all data backup processes. (PCI DSS Requirement 12.10.1)
* The IRP must contain an analysis of all legal requirements for reporting compromises of cardholder data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California residents data). (PCI DSS Requirement 12.10.1)
* The IRP must address coverage and responses for all critical system components. (PCI DSS Requirement 12.10.1)
* The IRP must include or reference the specific incident response procedures from the payment brands. (PCI DSS Requirement 12.10.1)
* The IRP must be tested at least annually and evidence maintained that can be used to validate annual testing is being performed per defined policies. (PCI DSS Requirement 12.10.2)
* SpeedPro Greenville must designate specific personnel to be available on a 24/7 basis to respond to alerts. This 24/7 coverage needs to include incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or application file changes. (PCI DSS Requirement 12.10.3)
* Require that staff with security breach responsibilities (as defined in the IRP) is periodically trained on their response procedures. (PCI DSS Requirement 12.10.4)
* A detailed process and/or procedure for monitoring and responding to alerts from security monitoring systems, including detection of wireless access points, must be defined and documented in the IRP. (PCI DSS Requirement 12.10.5)
* A process must be in place for modifying and evolving the IRP according to lessons learned and integrating best practices as the industry develops. (PCI DSS Requirement 12.10.6)

### 12.11 Internal Auditing of Critical Processes

* A quarterly assessment to verify personnel are following security policies and operating procedures will be performed, documented, and signed off by management. (PCI DSS Requirement 12.11)

# Appendix A – Management Roles and Responsibilities

## Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

### Table A1 - Management Security Responsibilities

| **Name of Role, Group, or Department** | **Date Assigned** | **Description of Responsibility** |
| --- | --- | --- |
|  |  | Establish, document, and distribute security policies |
|  |  | Monitor, analyze, and distribute security alerts and information |
|  |  | Establish, document, and distribute security incident response and escalation policies |
|  |  | Administration of user accounts on systems in the cardholder data network |
|  |  | Monitor and control all access to cardholder data |

## Appendix B – Agreement to ComplyAgreement to Comply with Information Security Policies

All employees working with cardholder data must submit a signed paper copy of this form. SpeedPro Greenville management will not accept modifications to the terms and conditions of this agreement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Department

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Telephone Number

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that SpeedPro Greenville internal information, or information that has been entrusted to SpeedPro Greenville by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with SpeedPro Greenville, I agree to return to SpeedPro Greenville all information to which I have had access as a result of my position with SpeedPro Greenville. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal SpeedPro Greenville manager who is the designated information owner.

I have access to a copy of the SpeedPro Greenville Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at SpeedPro Greenville, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from SpeedPro Greenville, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the SpeedPro Greenville Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to <the director of the Information Security department or identified responsible team, group, etc.>.  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature

1. See the Firewall and Router Configuration Standards document. [↑](#footnote-ref-1)
2. See the *System Hardening and Configuration Standards* document. [↑](#footnote-ref-2)
3. See the *Data Retention and Storage Procedures* document. [↑](#footnote-ref-3)
4. See the *Authorized Users List* document [↑](#footnote-ref-4)
5. See the *Data Encryption and Key Management Procedures* document. [↑](#footnote-ref-5)
6. See the *Vulnerability Discovery and Risk Ranking Process* document. [↑](#footnote-ref-6)
7. See the *Software Development Life Cycle Process* document. [↑](#footnote-ref-7)
8. See the *Physical Security Procedures* document. [↑](#footnote-ref-8)
9. See the *Physical Security Procedures* document. [↑](#footnote-ref-9)
10. See the *Physical Security Procedures* document. [↑](#footnote-ref-10)
11. See the *NTP Configuration Procedures* document. [↑](#footnote-ref-11)
12. See the *Risk Assessment Process* document. [↑](#footnote-ref-12)
13. See the *Operating Procedures* document. [↑](#footnote-ref-13)
14. See the *Operating Procedures* document. [↑](#footnote-ref-14)
15. See the *Risk Assessment Process* document. [↑](#footnote-ref-15)
16. See the *Critical Technology Device Inventory* document. [↑](#footnote-ref-16)
17. See the *Employee Computer Usage Policy* document. [↑](#footnote-ref-17)
18. See the *Security Awareness Training Process* document. [↑](#footnote-ref-18)
19. See the *Full Service Provider Compliance Validation Process* document. [↑](#footnote-ref-19)
20. See the *Full Service Provider Compliance Validation Process* document. [↑](#footnote-ref-20)
21. See the *Full Service Provider Compliance Validation Process* document. [↑](#footnote-ref-21)
22. See the *Incident Response Plan* document. [↑](#footnote-ref-22)