[Put your company logo here]

<MerchantName>

Information Security Policy for

SAQ P2PE Merchants

# About this Document

This document contains the <MerchantName> 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 PCI DSS Compliance – SAQ P2PE 1

About this Document 2

Table 1 - Revision History 2

Introduction 5

Purpose / Scope 5

Security Policy Ownership and Responsibilities 6

Additional Process and Standards Documents Referenced by this Security Policy 7

Table 2 – Security Process and Standards Documents Referenced by Policy 7

Protect Stored Cardholder Data 8

3 Protect Stored Data 8

3.1 Retention and Disposal of Sensitive Credit Card Account Data 8

3.2 Storage of Sensitive Credit Card Authentication Data 8

3.7 Security Policies and Operational Procedures Documentation 8

Implement Strong Access Control Measures 9

9 Restrict Physical Access to Cardholder Data 9

9.5 Physically Secure All Media 9

9.8 Media Destruction Policies and Procedures 9

9.9 Protection from Tampering and Substitution 9

9.10 Security Policies and Operational Procedures Documentation 10

Maintain an Information Security Policy 10

12 Maintain a Security Policy that Addresses Information Security for All Personnel 10

12.1 Publish, Distribute, and Update the Information Security Policy 10

12.4 Assign Information Security Responsibilities 10

12.5 Assign Information Security Management 10

12.6 Security Awareness Program 11

12.8 Policies for Sharing Data with Service Providers 11

12.10 Incident Response Plan Policies 11

Appendix A – Management Roles and Responsibilities 12

Assignment of Management Roles and Responsibilities for Security 12

Table A1 - Management Security Responsibilities 12

Appendix B – Agreement to ComplyAgreement to Comply with Information Security Policies 13

# Introduction

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

<MerchantName> 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 <MerchantName>‘s information technology resources. It is the responsibility of employees, contractors, business partners, and agents of <MerchantName>. Each should become familiar with this policy's provisions and the importance of adhering to it when using <MerchantName>‘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 <Name of the Information Technology Organization at the entity>.

# 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 <MerchantName>‘s information technology resources. The policy assigns responsibility and provides guidelines to protect <MerchantName>‘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 <MerchantName>‘s data network. It may apply to users of information services operated or administered by <MerchantName> (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with <MerchantName> are subject to these same definitions and rules when they are using <MerchantName>‘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 <MerchantName>’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 <Roles/Titles> is/are the assigned custodian(s) of this Security Policy. It is the responsibility of the custodian(s) of this security policy to publish and disseminate these policies to all relevant <MerchantName> 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 <MerchantName> 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 <MerchantName> security policies relating to the protection of sensitive data and particularly credit card data. Details on <MerchantName> 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 <MerchantName> 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** |
| --- | --- |
| Full Data Retention and Storage Procedures | <Custodian or Location> |
| Physical Security Procedures | <Custodian or Location> |
| Security Awareness Training Process | <Custodian or Location> |
| Service Provider Compliance Validation Process | <Custodian or Location> |
| Incident Response Plan | <Custodian or Location> |
| Operating Procedures | <Custodian or Location> |
| Risk Assessment Process | <Custodian or Location> |

# 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 <MerchantName> data storage standards and procedures[[1]](#footnote-1). 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).
* <MerchantName> 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 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).

### 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)

# 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”.

## 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.

### 9.5 Physically Secure All Media

* <MerchantName> will define specific procedures[[2]](#footnote-2) 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)

### 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)
* <MerchantName> must define and document specific procedures[[3]](#footnote-3) 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)
* 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

* 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)

# 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 <MerchantName> 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 <MerchantName> 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

* <MerchantName> 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 <MerchantName> 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)

### 12.4 Assign Information Security Responsibilities

* The <MerchantName>‘s information security policy and procedures apply to all employees (full, part-time, or work study employees), contractors, and individuals providing services for <MerchantName> and could affect security of cardholder information. (PCI DSS Requirement 12.4)

### 12.5 Assign Information Security Management

* + 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)

### 12.6 Security Awareness Program

* A formal security awareness program[[4]](#footnote-4) must exist and participation is required for all employees working within the cardholder data environment. (PCI DSS Requirement 12.6.a)

### 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 <MerchantName>’s behalf. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy.
* <MerchantName> shall maintain a documented list[[5]](#footnote-5) 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 <MerchantName>, 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[[6]](#footnote-6) should be followed. (PCI DSS Requirement 12.8.3)
* <MerchantName> shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance. (PCI DSS Requirement 12.8.4)
* <MerchantName> shall maintain a list[[7]](#footnote-7) of which PCI DSS requirements are managed by each service provider, and which are managed by <MerchantName>. (PCI DSS Requirement 12.8.5)

### 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 <MerchantName> IRP[[8]](#footnote-8):

* <MerchantName> must maintain a documented IRP and be prepared to respond immediately to a system breach. (PCI DSS Requirement 12.10)

# 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. <MerchantName> 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 <MerchantName> internal information, or information that has been entrusted to <MerchantName> by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with <MerchantName>, I agree to return to <MerchantName> all information to which I have had access as a result of my position with <MerchantName>. 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 <MerchantName> manager who is the designated information owner.

I have access to a copy of the <MerchantName> 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 <MerchantName>, 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 <MerchantName>, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the <MerchantName> 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 *Data Retention and Storage Procedures* document. [↑](#footnote-ref-1)
2. See the *Physical Security Procedures* document. [↑](#footnote-ref-2)
3. See the *Physical Security Procedures* document. [↑](#footnote-ref-3)
4. See the *Security Awareness Training Process* document. [↑](#footnote-ref-4)
5. See the *Service Provider Compliance Validation Process* document. [↑](#footnote-ref-5)
6. See the *Service Provider Compliance Validation Process* document. [↑](#footnote-ref-6)
7. See the *Service Provider Compliance Validation Process* document. [↑](#footnote-ref-7)
8. See the *Incident Response Plan* document. [↑](#footnote-ref-8)