SAQ P2PE Policy Template

Template Instructions: The content within this document is intended to serve as a starting point for organizations wishing to institute a PCI compliance policy for SAQ P2PE. Any and all sections can be utilized and adapted to align with the individual organization's objectives.

Disclaimer: While this template was created by a PCI Qualified Security Assessor (QSA), its intended use is for informational purposes only. ControlScan is not responsible for the use of the language herein for any organization's security or compliance policy documentation. All liability with respect to actions taken or not taken based on any of the content in this document is hereby expressly disclaimed.

SAQ P2PE Policy for <COMPANY>

Document Purpose

The purpose of this policy is to establish a security posture for the interaction of cardholder data and reduce the burden of the implementation and management of PCI of applicable controls required by the most current version of the Payment Card Industry Data Security Standard (PCI DSS).

Unless otherwise provisioned, documented, or communicated, this document establishes policy as it relates to the storage, processing, or transmission of cardholder data within <COMPANY>.

Scope

This document applies to all employees, contractors, and third party entities that store, process, transmit cardholder data, or otherwise interact with cardholder data which is processed against any transaction where <COMPANY> owns or is responsible for the associated merchant ID (MID). Furthermore, this policy applies to all devices that are used for the physical capture of cardholder data used to capture those transactions.

Statement of Policy

Unless otherwise approved by <COMPANY> leadership, the following policy must be implemented and managed.

Transaction Processing

1. All payment processing must be facilitated through a validated PCI P2PE solution approved and listed by the PCI Security Standards Council (SSC). No other forms of transaction processing will be permitted or approved.
2. <COMPANY> may not receive or transmit cardholder data electronically outside of a validated P2PE solution.

PCI P2PE Devices

1. All devices must be deployed in accordance with the vendor provided P2PE Implementation Guide.
2. Care, custody, and control must be applied to each device used to interact with cardholder data. These processes must include, but are not limited to, the following:
    a. Inventory management
        i. A formal inventory of all P2PE payment devices must be maintained.
        ii. A formal process to maintain this list must be implemented. This will include asset management of devices in production, inventory, reallocation, and decommissioning.
        iii. A formal inspection process must be implemented to ensure that there has not been any unauthorized substitution.
        iv. A formal list of each device must be maintained. This list will include, but is not limited to:
            1. Make and model of device
            2. Location of device
            3. Unique identifier
    b. Device security
        i. Devices must be inspected on a <Frequency> basis. This inspection must be sufficient to identify a tampered device.

Employee Training

1. Individuals must receive training sufficient to:
    a. Identify any payment device which has been tamped with.
    b. Be aware of suspicious behavior around payment devices.
    c. Be aware of devices which have been tamped with or substituted.
    d. Verify the identity of any individual claiming to provide repair or maintenance services.
    e. Not install, replace, or return devices without formal verification and approval by <Individual or Team>.
    f. Report any suspicious behavior to <Individual or Team>.
    g. Follow formal processes for inspection of any payment device used for cardholder data.
    h. Maintain the established frequency of inspection of payment devices.

Cardholder Data Storage

1. Storage of electronic/digital cardholder data is prohibited, unless required for documented legal reasons.
2. Storage of sensitive authentication data after authorization is prohibited.
3. Storage of physical print media is permitted, given the following requirements are met:
    a. A formal data retention policy must exist that defines the data that is retained, and the purpose of the retention. This retention must be defined with specific legal and/or business reasons.
    b. Physical print media containing cardholder data may not be stored for longer than its defined retention period.
    c. There must be a formal process, executed quarterly, to identify any data which has exceeded the retention period.
    d. In the event cardholder data has been identified as exceeding its retention period, a formal process must be implemented to securely dispose of it. Destroyed data should not be able to be recovered or reconstructed.
4. Storage of physical print media must be secured from any unauthorized access.

Policy Application

The application of this policy:

1. Must have procedures and standards clearly defined and documented to support the policy requirements.
2. Must establish processes to ensure this policy is in place and functioning.
3. Must ensure that this policy and supporting information is known and understood by all individuals within its scope.
4. Must include a formal review of this policy at least annually or when there is a significant change to business.
5. Must include an audit of the application of this policy at least every <Frequency>.
6. Must include an organization report of the adherence of this policy, reported to <Individual or Team> on a <Frequency> basis.