SAQ A 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 A. 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 A 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).

Statement of Policy

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

Transaction Processing

All storage, processing, or transmission of cardholder data must be outsourced to a PCI Compliant third party. <COMPANY> may not store, process, or transmit cardholder data outside of the relationships established with the third party to perform those activities on <COMPANY>'s behalf.

Cardholder Data Storage

- Electronic
  - <COMPANY> may not store electronic cardholder data information in any format on any medium for any amount of time.
  - <COMPANY> may not take custody of any cardholder data in within its premises.
- Written or Printed
  - <COMPANY> may store cardholder data in written or printed format for a period of time that does not exceed business or legal reasons.
  - Written or Printed cardholder data may not be received via electronic format.
  - A written media retention policy must be maintained that defines:
    - The length of time physical media may be retained.
    - The reason (business or legal) for the retention of physical media.
    - Acceptable methods of data destruction (cut shredded, incinerated, or pulped). Media which has been destroyed must not be recoverable.
  - Containers containing media containing cardholder information must be secure in such a way as to prevent unauthorized access.

Technical Controls

- System Configurations
  - All vendor-supplied defaults must be changed before installing onto <COMPANY> system or network.
  - All unnecessary default accounts must be removed or disabled before installing any system onto the network.
- Vulnerability Management
  - All system components and software must be protected from known vulnerabilities by installing critical security patches within one month of release.
- Authentication
  - All users are assigned a unique ID on any system they access.
  - All user access must be immediately deactivated or removed upon termination.
  - All users must be authenticated using their unique ID and one of the following attributes:
    - Something they know
    - Something they have
    - Something they are
  - Passwords must meet the following minimum requirements:
    - At least seven (7) characters
    - Contain both Alpha and Numeric values/characters
  - Group/shared/generic accounts and passwords are strictly prohibited.

Physical Controls

All physical media containing cardholder data must be secure from unauthorized access.

- Distribution of any physical media containing cardholder data must be strictly maintained. This maintenance must include the following:
    - Media classification
    - Methods to track its location and sent via secure courier
    - Media inventories
    - Physical access controls
    - Management's approval for its movement
    - Media destruction when it has exceeded its retention period. Once destroyed, media may not be recoverable.

Incident Response

In the event <COMPANY> is notified that there has been a security incident relating to the security of any cardholder data processed, stored, or transmitted against <COMPANY>'s MID, <COMPANY> must implement a formal incident response program. This program must be developed and maintained according to industry standards and best practices.

Service Provider Management

A formal program must be established and maintained to ensure that any third party that has access to cardholder on behalf of <COMPANY> are doing things in a PCI complaint manner. This program will require the following vendor management procedures to be established.

- A formal list of any third-party entity that stores, processes, or transmits cardholder data on behalf of <COMPANY> or otherwise would have the ability to impact the cardholder data security must be maintained.
- A written agreement must be maintained between <COMPANY> and any third party that stores, processes, or transmits cardholder data on behalf of <COMPANY> or otherwise would have the ability to impact the cardholder data. This agreement must contain acknowledgements between <COMPANY> and the third party which denotes that the third party will agree to maintain all applicable PCI DSS controls in a PCI complaint way.
- Formal due diligence must be document and established before allowing any third-party access to <COMPANY> cardholder data or otherwise interacting with it. This process must establish that the third party has the ability to obtain and retain the applicable PCI DSS controls such that this party will not impose a security risk to the cardholder data.

- <COMPANY> must develop a formal program to ensure that any third party which stores, processes, or transmits cardholder data on behalf of <COMPANY> or otherwise would have the ability to impact the cardholder data is PCI DSS compliant. Vetting of third parties must be done at least annually.
- A formal list of controls for any third party that stores, processes, or transmits cardholder data on behalf of <COMPANY>, or otherwise would have the ability to impact the cardholder data, must be maintained. This list must contain controls that the third party is responsible to maintain, the list of controls <COMPANY> is responsible for, and those which have a shared obligation to be maintained.

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.