ControlScan

SAQ A-EP 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-EP. 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-EP 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.

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 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.

- Sensitive Authentication Data may not be stored after authorization under any circumstance.

Technical Controls

- Network management
  - Documented configuration standards must be maintained.
  - A list of all permitted services and ports must be maintained. Where there is a required protocol that is known to be vulnerable, controls must be documented, implemented, and maintained to render the risky nature of the protocol mute.
  - Any change to any firewall or router must be conducted in accordance with <COMPANY> change control procedures.
  - Network and dataflow diagrams must be kept current and demonstrate flows across all systems and networks.
  - A firewall must be maintained between any cardholder data environment (CDE) and the Internet.
  - Firewall and router rules must be reviewed at least every six months. This review is to ensure that any protocol, port, or services permitted continues to be secure, the ports are still required and approved by management, and the configurations are in a known state.
  - Firewalls must be configured to only allow protocols and ports that are approved by management. This includes both inbound and outbound ports from the CDE to any other location. All other ports and services not documented and approved must be explicitly denied.
  - Router and firewall configurations must be secure from unauthorized access.
  - Startup configurations must be synchronized with running configurations at any point a network configuration is altered.
  - Anti-spoofing and stateful inspection must be configured and enabled on all border firewalls and routers.
  - Outside traffic must be limited to only IP addresses within the CDE and only to those systems that are required to be publicly facing to provide public services. All other inbound traffic must be denied.
  - All internal systems must be configured to prevent the disclosure of the internal IP space of the internal/private systems. Any disclosure of this IP space must be approved by management.

- Any portable or employee-owned system that connects to both the CDE and the Internet, does not need to be at the same time, must have a personal firewall configured and enabled. This firewall cannot be disabled or reconfigured by the end user. The configuration of the personal firewalls must be documented and maintained.

- 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.
  - Configuration standards must be created and maintained for all assets. These standards must be developed based on industry best practices and maintained to ensure new systems going into production are free from known vulnerabilities.
    - Configuration standards must be applied before assets are put into production.
    - These standards must, at a minimum, require the following security attributes:
      - Changing of all vendor-supplied defaults and elimination of unnecessary default accounts
      - Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server
      - Enabling only necessary services, protocols, daemons, etc., as required for the function of the system
      - Implementing additional security features for any required services, protocols or daemons that are considered to be insecure
      - Configuring system security parameters to prevent misuse
      - Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers
  - All remote, non-console administrative access must be encrypted using secure protocols. Encryption must be established before any administrative password is requested.
  - All systems must be maintained from malware.
    - A solution must be implemented and maintained to prevent systems from being impacted by malware.
    - Scans for malware must be completed at a frequency to address risk as documented within the <COMPANY> risk assessment.
    - Anti-malware solution may not be disabled by end users unless specifically authorized by management, for a specific reason, for a specific period of time.
    - Malware solutions must generate and maintain logs in accordance with <COMPANY> logging requirements.

- Secure Data Transmission
    - Any transmission of cardholder data must be done under the following requirements:
        - Strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks
        - Only trusted keys are accepted
        - Security protocols implemented to use only secure configurations, and to not support insecure versions or configurations
        - Proper encryption strength implemented for the encryption methodology in use
        - TLS 1.0 or any version of TLS may not be used
    - Cardholder data may not be sent over end-user messaging protocols in an unencrypted state.
- Vulnerability Management
    - Formal processes must be implemented to identify security vulnerabilities. These processes must include reputable outside third parties and a process to rank any identified vulnerability.
    - All systems components and software must be protected from known vulnerabilities by installing critical security patches within one month of release.
    - Any change made that impacts a policy, procedures, standards, or an artifact that is required by the PCI DSS must be updated before the change is closed.
- 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.

Secure Software Management

- Any software developed or used to store, process, or transmit cardholder data must be developed and managed so that they are free from known coding vulnerabilities. At a minimum, this code must be free of:
    - Injection flaws
    - Buffer overflow
    - Insecure communications
    - Insecure error handling
    - High-ranking vulnerabilities as identified in the vulnerability identification program
    - Cross-site scripting
    - Insecure direct object reference

  - Cross-site request forgery
  - Broken authentication
- For any public-facing, web-based application, one of the following processes must be implemented.
  - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows:
    - At least annually
    - After any changes
    - By an organization that specializes in application security
    - That, at a minimum, all vulnerabilities in PCI DSS Requirement 6.5 are included in the assessment
    - That all vulnerabilities are corrected
    - That the application is re-evaluated after the corrections

    –OR–

  - Install an automated technical solution that detects and prevents web-based attacks (for example, a web application firewall or WAF) as follows:
    - Is situated in front of public-facing web applications to detect and prevent web-based attacks
    - Is actively running and up to date as applicable
    - Is generating audit logs
    - Is configured to either block web-based attacks or generate an alert that is immediately investigated

Change Control

- <COMPANY> must formally implement a documented change control program that includes the following attributes:
  - Documentation of impact
  - Documented change control approval by authorized parties
  - Functionality testing to verify that the change does not adversely impact the security of the system
  - Back-out procedures

Authorization

Access to system components and cardholder data is limited to only those individuals whose jobs require such access.

- Access to systems must be permitted on the least privileges necessary for the individual to perform their job; however, the individual may not have more access or permissions than what is required.
- All access must be granted based on the individual's job classification and function.
- All access to any system must be approved by management.

Authentication

<COMPANY> must develop and maintain procedures to address the authentication of all in-scope systems. At a minimum, these procedures must be implemented:

- All individuals must have their own username and it may not be shared.
- Default, shared, or generic user accounts may not be used or created.
- Processes must be established to manage the move, add, change of all user accounts. Any modification to any account must be monitored.
- All access to any terminated user must be removed or deactivated immediately.
- Accounts not used within a 90-day period must be disabled.
- Accounts used by third parties or vendors must be disabled when not in use and only enabled when required and in use.
- Account access attempts must be locked after six invalid attempts. If an account is locked, it must remain disabled for 30 min or until an admin resets the account.
- User sessions must time out after 15 minutes of nonuse and must require the user to reauthenticate.
- All non-console administrative access and all remote access may only be permitted through the use of multi-factor authentication.
- Authentication policy and procedures must be clearly defined and provided to all employees.
- Physical devices used for authentication may only be assigned to an individual and not a group.

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.
- Any place where physical media is stored, controls must be implemented to prevent unauthorized physical access.

Program Management

A security-knowledgeable member of management must be assisted reasonably for the overall management of the <COMPANY> PCI program. This individual is responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.

This individual or delegate will also be responsible for ensuring the daily activities associated with managing the PCI environment are performed.

Security Training

All staff subject to any control within the PCI DSS must have training on their specific roles and responsibilities. This training must be provided when the individual is first hired, and then again annually. This training must include the training on policy, procedures, and tasks required for the individual to perform their job.

Service Provider Management

A formal program must be established and maintained to ensure that any third party that has access to cardholder data on behalf of <CUSTOMER> is 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 denote that the third party will agree to maintain all applicable PCI DSS controls in a PCI complaint way.
- Formal due diligence must be documented 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 that 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.

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. At a minimum, the incident response program must include the following attributes:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment card brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment card brands

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 be provided to all individuals within its scope.
7. Must include an organizational report of the adherence of this policy, reported to <Individual or Team> on a <Frequency> basis.