INSTRUCTIONS:

This document is intended to aid someone in building a security policy for their company. It must be read and appropriately modified before it is suitable for use.

- Conduct a “Search and Replace” of the term “<MerchantName>” with the appropriate company name (this is necessary but insufficient to make this policy ready for use).
- Review all items in red text and take the appropriate action depending on the organization's business activities. For example, some statements apply to PCI controls that are future dated or only required of service providers and can be removed by a merchant.
    - Notes in red text are helpful instructions to the final user of this policy and should be deleted when no longer needed.
- Conduct a review of all the statements to make certain that the policy aligns with existing business processes, and to identify any existing business processes that need to be adjusted.
- Update any references in this policy to secondary documents (policies, standards, procedures) to make certain the reference herein contains the correct name of the secondary document.
- Complete all applicable appendices.

AMERICAN ALLIANCE OF PARALEGALS, INC. (AAPI)

Information Security Policy for SAQ A PCI DSS Compliance

About this Document

This document contains the American Alliance of Paralegals, Inc. 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
4.0	July 2022	MAH	Update for PCI DSS v4.0

Contents

Introduction

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

AAPI 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 AAPI‘s information technology resources. It is the responsibility of employees, contractors, business partners, and agents of AAPI. Each should become familiar with this policy's provisions and the importance of adhering to it when using AAPI‘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 President and Board of Directors of the American Alliance of Paralegals, Inc.

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 AAPI‘s information technology resources. The policy assigns responsibility and provides guidelines to protect AAPI‘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 AAPI‘s data network. It may apply to users of information services operated or administered by AAPI (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with AAPI are subject to these same definitions and rules when they are using AAPI‘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 Credit Card Data used by American Alliance of Paralegals, Inc. (AAPI).

Credit card data stored, processed or transmitted with AAPI’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 full Primary Account Number (PAN) which may also appear in conjunction with Cardholder Name, Service Code, or Expiration date. Sensitive Authentication Data within this document is defined as the Card Validation Code (CVC, CVV2, CID, CAV2 and CVC2), Credit Card PIN, and any form of magnetic stripe data from the card (Track 1, Track 2). Account Data within this document is defined by any combination of Cardholder Data and Sensitive Authentication Data.

Security Policy Ownership and Responsibilities

The President/Treasurer of the American Alliance of Paralegals, Inc. 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 AAPI 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 AAPI 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 AAPI security policies relating to the protection of sensitive data and particularly credit card data. Details on AAPI's 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 AAPI's 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
System Hardening and Configuration Standards	<Custodian or Location>
Full Data Retention and Storage Procedures	<Custodian or Location>
Vulnerability Discovery and Risk Ranking Process	<Custodian or Location>
Operating Procedures	<Custodian or Location>
Service Provider Compliance Validation Process	<Custodian or Location>
Incident Response Plan	<Custodian or Location>

2 Secure Configurations are applied to all system components

2.2 System components are configured and managed securely

In order to ensure system components are configured consistently and securely and reduce the opportunities available to an attacker, AAPI securely configures and manages system components as follows:

- Configuration standards[1] shall be developed, implemented, and maintained to:
    - Cover all system components.
    - Address all known security vulnerabilities.
    - Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.
    - Be updated as new vulnerability issues are identified, as defined in PCI DSS Requirement 6.3.1.
    - Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. (PCI DSS Requirement 2.2.1)
- When a vendor default account(s) is used, the default password should be changed per PCI DSS Requirement 8.3.6.
- If a vendor default account(s) is not used, the account should be removed or disabled. (PCI DSS Requirement 2.2.2)

Protect Stored Cardholder Data

Note: The following section applies to merchants with paper records that include stored cardholder account data (for example, receipts or printed reports).

3.1 Processes and mechanisms for protecting stored account data are defined and understood

AAPI ensures documented processes and mechanisms for applying secure configurations to all system components are defined and understood, as follows:

- All security policies and operational procedures that are identified in this section shall be documented, kept up to date, in use, and known to all affected parties. (PCI DSS Requirement 3.1.1)
- Roles and responsibilities for performing activities in this section shall be documented, assigned, and understood.[2]

3.2 Storage of account data is kept to a minimum

To ensure that sensitive data is securely destroyed or deleted as soon as it is no longer needed, AAPI

[1] System Hardening Standards

[2] PCI Security Roles and Responsibilities Matrix

maintains a formal data retention policy that identifies what data needs to be retained, for how long, and where that data resides, as follows:

- Account data storage shall be kept to a minimum through implementation of data retention and disposal policies, procedures, and processes[3] that include at least the following:
    - Coverage for all locations of stored account data.
    - Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.

      Note: The previous bullet is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.
    - Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
    - Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
    - Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
    - A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. (PCI DSS Requirement 3.2.1)

6 Development and Maintenance of Secure Systems and Software

All system components must have appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software

Appropriate software patches must be evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

6.3 Security Vulnerabilities are Identified and Addressed.

- AAPI will identify and manage security vulnerabilities as follows: New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs), vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact, risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment and vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. (PCI DSS Requirement 6.3.1)
- All system components are protected from known vulnerabilities by installing applicable security

[3] Data Retention Policy

patches/updates as follows: critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release and all other applicable security patches/updates are installed within an appropriate time frame as determined by AAPI (for example, within three months of release).(PCI DSS Requirement 6.3.3)

6.4 Protection of Public-Facing Web Applications Against Attacks

- All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: A method is implemented to confirm that each script is authorized, a method is implemented to assure the integrity of each script and an inventory of all scripts is maintained with written justification as to why each is necessary.(PCI DSS Requirement 6.4.3) Note: This is a future dated PCI DSS Requirement effective after 31 March 2025. This new requirement will replace Requirement 6.4.1 once its effective date is reached. (See PCI DSS Requirement 6.4.2 and 6.4.3). Please update this bullet point to reflect how your company is addressing this requirement and then remove this "Note".

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. Detailed authentication procedures should be developed and documented to meet the following policies.

8.2 User Identification and Related Accounts for Users and Administrators are Strictly Managed throughout an Account's Lifecycle

- Assign all users a unique ID before granting access to system components or cardholder data. (PCI DSS Requirement 8.2.1)
- Only use group, shared, or generic accounts, or other shared authentication credentials, when necessary, on an exception basis and manage as follows: (PCI DSS Requirement 8.2.2)
    - Account use is prevented unless needed for an exceptional circumstance.
    - Use is limited to the time needed for the exceptional circumstance.
    - Business justification for use is documented.
    - Use is explicitly approved by management.
    - Individual user identity is confirmed before access to an account is granted.
    - Every action taken is attributable to an individual user.
- Immediately revoke access for terminated users. (PCI DSS Requirement 8.2.5)

8.3 Authentication for Users and Administrators

- All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: (PCI DSS Requirement 8.3.1)
    - Something you know, like a password or passphrase.

- Something you have, like a token device or smart card.
- Something you are, like a biometric element.

- When passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: (PCI DSS Requirement 8.3.5)
  - Set to a unique value for first-time use and upon reset.
  - Forced to be changed immediately after the first use.
- When passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they must meet the following minimum level of complexity: (PCI DSS Requirement 8.3.6)
  - A minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of 8 characters).
  - Contain both numeric and alphabetic characters.
- Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases they have used. (PCI DSS Requirement 8.3.7)
- When passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: (PCI DSS Requirement 8.3.9)
  - Passwords/passphrases are changed at least once every 90 days, **OR**
  - The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.
  - Factors are assigned to an individual user and not shared among multiple users.
  - Physical and/or logical controls ensure only the intended account can use that factor to gain access.

9 Restrict Physical Access to Cardholder Data

Any physical access to locations that house cardholder data provide the opportunity for individuals to access data and to remove hardcopies and should be appropriately restricted. Detailed physical security procedures should be developed and documented to meet the following policies.

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 '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 media containing cardholder data.

9.4 Securely Store, Access, Distribute, and Destroy Media with Cardholder Data

- AAPI will define specific procedures[4] to physically secure all media, including but not limited to paper receipts, paper reports. (PCI DSS Requirement 9.4.1)

[4] See the *Physical Security Procedures* document.

- Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility and review the security of storage locations at least once every 12 months. (PCI DSS Requirement 9.4.1.1)
- Classify all media with cardholder data in accordance with the sensitivity of the data. (PCI DSS Requirement 9.4.2)
- Maintain strict control over the external distribution of media with cardholder data, including the following: (PCI DSS Requirement 9.4.3)
    - Media sent outside the facility is logged.
    - 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 with cardholder data that is moved from a secured area, including when media is distributed to individuals. (PCI DSS Requirement 9.4.4)
- Destroy hard-copy materials containing cardholder data when it is no longer needed for business or legal reasons, as follows: (PCI DSS Requirement 9.4.6)
    - Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
    - Materials are stored in secure storage containers prior to destruction.

11 Regularly Test Security Systems and Processes

Vulnerabilities are continually being introduced by new software and discovered in current software. System components, processes, and bespoke and custom software must be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures[5] should be developed and documented to meet the following policies.

11.3 Vulnerability Assessment Scans

- External vulnerability assessment scans must be performed at least every three months and after any significant change in the cardholder data environment (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). (PCI DSS Requirement 11.3)
- External vulnerability scans must (PCI DSS Requirement 11.3.2)
    - Be performed at least every three months, and after any significant change.
    - Be performed by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC), or by qualified personnel (if the scan is performed after any significant change).
    - Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

[5] See the *Operating Procedures* document.

- 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 11.3)

- Ensure that results of each quarter's internal and external vulnerability assessments are to be documented and retained for review. (PCI DSS Requirement 11.3)

11.6 Change Detection on Payment Pages

- Deploy a change-detection mechanism to alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. This mechanism is configured to evaluate the received HTTP header and payment page at least once every seven days or periodically at a defined frequency that is the result of targeted risk analysis which is performed according to all elements specified in Requirement 12.3.1. (PCI DSS Requirement 11.6.1) Note: This is a future dated PCI DSS Requirement effective after 31 March 2025. Please update this bullet point to reflect how your company is addressing this requirement and then remove this "Note".

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 AAPI security policies described in this document.

12 Support Information Security with Organizational Policies and Programs

A strong security policy sets the security tone for AAPI 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:** For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of account data.

12.8 Policies for Working with Third Party Service Providers (TPSPs)

- 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 AAPI's behalf. Service providers, which could affect the Cardholder Data, are also in-scope of this policy.
  - AAPI shall maintain a documented list[6] of all applicable service providers in use and the services they provide. (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

6

they receive from or on behalf of AAPI, 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[7] should be followed. (PCI DSS Requirement 12.8.3)

- AAPI shall review the PCI DSS attestation of compliance form(s) for its third-party service providers and confirmed that the third-party service providers are PCI DSS compliant for the services being used by the merchant. (PCI DSS Requirement 12.8.4).
- AAPI shall maintain a list[8] of which PCI DSS requirements are managed by each service provider, which are managed by AAPI, and any that are shared between the service provider and AAPI. (PCI DSS Requirement 12.8.5)

12.10 Incident Response Plan Policies

Incidents or suspected incidents regarding the security of the Cardholder Data Environment 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 AAPI IRP[9]:

- AAPI 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 contact/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 for different types of incidents. (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

[7] See the *Service Provider Compliance Validation Process* document.

[8] See the *Service Provider Compliance Validation Process* document.

[9] See the *Incident Response Plan* document.

brands. (PCI DSS Requirement 12.10.1)

- 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 environment
		Monitor and control all access to cardholder data

Appendix B – Agreement to Comply

Agreement to Comply with Information Security Policies

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

John C. Goudie

_____

Employee's Printed Name

Treasurer – American Alliance of Paralegals, Inc.

_____

Employee's Department

414-630-1716

_____

Employee's Telephone Number

4023 Kennett Pike, Suite 146

Wilmington, DE 19807-2018

_____

Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that AAPI's internal information, or information that has been entrusted to AAPI by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with AAPI, I agree to return to AAPI all information to which I have had access as a result of my position with AAPI. 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 AAPI manager who is the designated information owner.

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

I agree to choose a difficult-to-guess password as described in the AAPI 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 President and Board of Directors.

John C. Goudie, AACP

_____

Employee's Signature

