**Paz & Associates Privacy and Information Security Policies**

# Privacy Policy

Respect for the privacy, security, and confidentiality of clients is our utmost concern. The purpose of this privacy policy is to let you know how we use personal information collected via website, phone or fax. Please note that the practices set forth in this privacy policy apply to Paz & Associates only. If you link to other web sites or talk with other vendors, please review their own respective privacy policies.

## Collection of Information

When voluntarily submitted by visitors to our website, we collect certain information like names, postal addresses, email addresses, phone number, etc. The information you provide is used to fulfill your specific request or order, and allows us to add you to one of our mailing lists.

## Distribution of Information

We may share information with book industry-related organizations or our training partners, who may or may not use the information for marketing purposes. We may also share information when trying to protect against or prevent actual or potential fraud or unauthorized transactions.

## Commitment to Data Security

Your personally identifiable information is kept secure. Only Paz & Associates representatives and contractors (who have agreed to keep information secure and confidential) have access to this information. All communications via Constant Contact allow you to opt out of further mailings.

## Privacy Contact Information

If you have any questions, concerns, or comments about our privacy policy you may contact us using the information below:

By e-mail: dpaz@pazbookbiz.com
By Phone: (904) 277-2664

Thank you for placing your trust and confidence in Paz & Associates to facilitate your bookstore dreams.

# Security Policy

**Overview**

This policy is intended to relay the importance of security and protecting cardholder data.

**Purpose**

- To establish the Paz & Associates policy for the secure handling of sensitive card holder data including but not limited to magnetic strip data, Primary Account Numbers (PAN's), expiration date, and service code

**Scope**

This policy applies to all employees and systems of Paz & Associates

**Policies to Protect and Manage Cardholder Data**

The importance of protecting cardholder data is paramount. Allowing data theft or destruction, inadvertently sharing confidential information, infecting system networks with viruses, misuse of company resources, allowing the theft of company property, and allowing the compromise of private or confidential company or client information are all very real examples of what might result from a security compromise.

1.0 Strong cryptography and security protocols, such as SSL, TLS or IPSEC, are to be used to safeguard sensitive cardholder data during transmission over open, public networks.

2.0 All sending of unencrypted Primary Account Numbers by end-user messaging technologies (i.e., email, instant messaging, and chat) are strictly prohibited. If a PAN must be sent by end-user messaging, only email is allowed and the PAN will be encrypted using WinZip. The WinZip password will be communicated to the end user by means other than end user messaging (phone or fax is allowed).

3.0 Access to system components and cardholder data is limited to only those authorized individuals whose job require such access or have a need-to-know. This authority is granted by senior management and reviewed annually.

4.0 All paper that contains cardholder data is to be identified and physically secured in a locked drawer. No electronic cardholder data will ever be stored.

5.0 Strict control is to be maintained over the internal or external distribution of any kind of media that contains cardholder data

- Media is classified and clearly marked as confidential
- Media is sent by secured courier or other delivery method that can be accurately tracked

6.0 Management approval is to be obtained prior to moving any and all media containing cardholder data from a secured area.

7.0 Strict control must be maintained over the storage and accessibility of media that contains cardholder data.

8.0 Media containing cardholder data is to be destroyed when it is no longer needed for business or legal reasons.

- Paper materials are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
- The general rule is that media containing cardholder date will be destroyed when over 180 days old. Exceptions to the rule must be approved by senior management.

**Policy Maintenance and Employee/Contractor Awareness**

1.0 Review of this policy will be conducted on an annual basis or as changes to the environment occur

2.0 Usage of employee-facing technologies such as remote access, wireless, electronic media, internet, PDA's and wireless will adhere to the following:

- No unauthorized equipment can be brought in or set up in Paz & Associates facility. This includes, but is not limited to modems, computers, or wireless devices.

- Wireless devices must be set up securely by establishing secure accounts/passwords, disabling SSID broadcasts, and using the highest available encryption for the device.

3.0 One or more employees will be designated with security responsibility.

4.0 Incident response documents will be created, reviewed by all employees, and will be updated on an annual basis.

5.0 These security policies will be formally reviewed annually with all employees/contractors.

6.0 A list of Service Providers must be maintained. This list will be updated and reviewed by senior management when necessary but at every 180 days.

7.0 A written Agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider posses is required from each Service Provider.

8.0 Due diligence is to be performed prior to the engagement of Service Providers. Procedures performed will include when possible:

- A visit to the Service Providers physical offices to discuss security practices and procedure with their management and staff.
- A written statement acknowledging their responsibilities to securely process, handle and transmit cardholder data.
- Written proof that the Service Provider is PCI compliant.
- Request reliable industry references.

9.0 A program is to be maintained to monitor Service Providers' PCI DSS compliance status. On an annual basis a request for a new compliance certificate will be requested.

# CERTIFICATE OF VALIDATION

## THIS CERTIFIES THAT

## Paz & Associates

HAS COMPLETED ALL SECTIONS OF
THE PAYMENT CARD INDUSTRY'S SELF ASSESSMENT QUESTIONNAIRE
RESULTING IN A COMPLIANT RATING

**Validation Date:** 14TH DAY OF MAY 2014

**Validation Number:** IPMT42236982002805380514



***Expiration Date:** 14TH DAY OF MAY 2015


*All merchants are required to validate their PCI compliance yearly. The overall PCI status could be affected by changes in the merchants card processing environment and/or failure to provide a passing scan as outlined in requirement 11.2 of the PCI Security Standard should one be required.