ABATE of Alaska, Inc.
"Riders of the Last Frontier"

Policies & Procedures

Version 2.0 - January 07, 2021

TABLE OF CONTENTS

1 REVISION HISTORY

Changes	Approving Authority	Date
Initial Publication	ABATE of Alaska Board of Directors	02/02/2017
Added Elections Policy and Vice-President Procedures	ABATE of Alaska Board of Directors	10/11/2018
Updated Elections Policy & Procedures	ABATE of Alaska Board of Directors	11/07/2019
Version 2.0 – Statewide Organization	ABATE of Alaska Board of Directors	01/01/2021

2 OVERVIEW

ABATE of Alaska Inc.'s Policies and Procedures

Introduction

This document explains ABATE of Alaska, Inc.'s Policies and Procedures for anyone that may represent ABATE of Alaska, Inc. while assisting at event booths, trade shows, or other public functions. ABATE of Alaska, Inc.'s management is committed to these policies to protect the organization and information utilized by ABATE of Alaska, Inc. in attaining its business goals. All Board Members, Officers, Members, Contractors, and Volunteers are to be made aware of these policies and procedures and required to adhere to them as described within this document.

Scope of Compliance

These Policies and Procedures apply to all Board Members, Officers, Members, Contractors, and Volunteers assisting with and participating in events representing ABATE of Alaska, Inc.

The requirements and procedures outlined below are intended to educate and protect ABATE of Alaska, Inc. and its volunteers who may be acting on behalf of, volunteering for, or otherwise representing ABATE of Alaska, Inc.

Requirements

ABATE of Alaska Policies and Procedures

ABATE of Alaska, Inc. maintains these Policies and Procedures that have been approved by the ABATE of Alaska, Inc. Board of Directors. New individual policies must be approved by the Board prior to being added to this document. All additions and changes will be noted in the Revision History section.

Summary

Responsibilities

In the event of a violation of these policies and procedures, the Board or its designee will determine the proper response and/or action. Designees may include, but are not limited to any Executive Officer, Board Member, or Event Coordinator as the Board determines is appropriate.

3 CONFLICT OF INTEREST POLICY

Introduction and Scope

Introduction

This document explains the conflict of interest policy for ABATE of Alaska, Inc. ABATE of Alaska, Inc.'s management is committed to these policies to protect the organization and information utilized by ABATE of Alaska, Inc. in attaining its business goals. All Board Members, Officers, Members, Contractors, and Volunteers are required to adhere to the policies described within this document.

Scope of Compliance

These election conflict of interest policies apply to all Board Members, Officers, Members, Contractors, and Volunteers assisting with and participating in events representing ABATE of Alaska, Inc. as may be applicable.

The requirements and procedures outlined below are intended to educate and protect ABATE of Alaska, Inc. and its volunteers who may be processing transactions or accepting donations on behalf of ABATE of Alaska, Inc.

Requirement 1: Obligations and Conduct

Inurement

A. Officers, Directors, and Board Members of ABATE of Alaska, Inc. are obligated to always act in the best interest of the ABATE of Alaska, Inc. This obligation requires that any officer, director, or board member in the performance of organizational duties, seek only the furtherance of the organization's mission. At all times, officers, directors, and board members are prohibited from using their job title or the organization's name or property, for private profit or benefit.

   1. The officers, directors, and board members of ABATE of Alaska, Inc. should neither solicit nor accept gratuities, favors, or anything of monetary value from contractors/vendors. This is not intended to preclude bona-fide organization fund raising-activities.
   2. No officer, director, or board member of ABATE of Alaska, Inc. shall participate in the selection, award, or administration of a purchase or contract with a vendor where, to his knowledge, any of the following has a financial interest in that purchase or contract:

      1. The officer or board member;

      2. Any member of their immediate family;

      3. Their partner;

      4. An organization in which any of the above is an officer, director or employee;

      5. A person or organization with whom any of the above individuals is negotiating or has an arrangement concerning prospective employment.

Requirement 2: Notification

Disclosure

Any possible conflict of interest shall be disclosed by the person or persons concerned as soon as reasonably possible to the ABATE of Alaska, Inc. Board of Directors.

Requirement 3: Board of Directors Activity

Board Action

When a conflict of interest is relevant to a matter requiring action by the ABATE of Alaska, Inc. Board of Directors, the interested person(s) shall call it to the attention of the Board and said person(s) shall recuse themselves from (not vote on) the matter. In addition, the person(s) shall not participate in the final decision or related deliberation regarding the matter under consideration. When there is a doubt as to whether a conflict exists, the matter shall be resolved by vote of the Board, excluding the person(s) concerning whose situation the doubt has arisen.

Requirement 4: Board Meeting Minutes

Record of Conflict

The official minutes of the Board shall reflect that the conflict of interest was disclosed and the interested person(s) did not participate in the final discussion or vote and did not vote on the matter.

Summary

Overall Conduct and Obligations

As noted in **Requirement 1** above, all Board Members, Officers, Members, Contractors, and Volunteers for ABATE of Alaska, Inc. are expected to conduct themselves in a professional and courteous manner when representing ABATE of Alaska, Inc. This expectation includes acting in the best interest of ABATE of Alaska, Inc. as a charitable, non-profit organization focusing on education and representation of all motorcycle riders throughout Alaska.

4 MEMBERSHIP POLICY

Introduction and Scope

This document explains ABATE of Alaska, Inc.'s Membership policy for anyone granted membership in ABATE of Alaska, Inc. All Board Members, Officers, Members, Contractors, and Volunteers are to be made aware of these policies and procedures and required to adhere to them as described within this document.

The following information further defines membership in ABATE of Alaska

Scope of Compliance

These Policies and Procedures apply to all Board Members, Officers, Members, Contractors, and Volunteers assisting with any membership coordination efforts while representing ABATE of Alaska, Inc.

The requirements and procedures outlined below are intended to educate and protect ABATE of Alaska, Inc. and its volunteers who may be acting on behalf of, volunteering for, or otherwise representing ABATE of Alaska, Inc.

Requirements

Membership Types

A. Charter Members. The initial members of any district chapter established by the Board of Directors whose dues are fully paid and the members of any new district chapter formed according to these Bylaws whose dues are fully paid and who become members of the district chapter within ninety (90) days after the chapter is granted its charter by the Board of Directors will be designated as charter members of that district chapter.

B. Regular Members. Any person who has applied for membership and has paid their dues for one year or more that has not been otherwise disqualified by the Board of Directors.

C. Lifetime Members. Any person who has been awarded a lifetime membership by the Board of Directors.

D. Honorary Members. The Board of Directors shall be authorized to grant Honorary membership to any person deemed worthy by the Board of Directors. Any such person shall be exempt from payment of dues, but shall have no vote in the affairs of the Corporation.

Termination of Membership

The membership of any member of the Corporation shall automatically terminate:

a. upon expiration of the membership term, unless renewed,
b. on written request by the member for such termination delivered to an officer of the Corporation personally or by United States mail;
c. upon suspension from membership in the Corporation of the member by four-fifths (4/5) vote of the Board of Directors for good cause, after the member having received written notice by U.S. Mail and the member having had an opportunity to be heard before the Board if the member has committed acts prejudicial to the purposes or welfare of this Corporation. The decision of the Board of Directors on termination of membership is final.

Management of Membership

Currently, ABATE of Alaska, Inc.'s Membership is managed through the Wild Apricot cloud application at **https://abateofalaska.wildapricot.org/**. A designated statewide Membership coordinator will be responsible for reviewing, managing, and maintaining the membership database. Chapter Membership Coordinators may also be assigned management roles within Wild Apricot.

Membership Chapters

Members of ABATE of Alaska, Inc. may also be members of a local chapter based on their physical residence address.

Membership Levels

The varying levels of Membership with their terms and their dues are follows:

Name Type	*Renewal period*	*Membership fee*	*Automatic recurring payments*	*Public can apply*
1 - One Year Individual Membership - AutoRenewing Individual	Every 1 year (starting from join date)	$25.00 (USD)	Yes	Yes
1 - One Year Individual Membership - NonAutoRenewing Individual	Every 1 year (starting from join date)	$25.00 (USD)	No	Yes
2 - Three Year Individual Membership Individual	Every 3 years (starting from join date)	$60.00 (USD)	No	Yes
3 - One Year Business Membership - AutoRenewing Individual	Every 1 year (starting from join date)	$60.00 (USD)	Yes	Yes
3 - One Year Business Membership - NonAutoRenewing Individual	Every 1 year (starting from join date)	$60.00 (USD)	No	Yes
4 - Three Year Business Membership Individual	Every 3 years (starting from join date)	$150.00 (USD)	No	Yes
5 - One Year Sustaining Membership - AutoRenewing Individual	Every 1 year (starting from join date)	$100.00 (USD)	Yes	Yes
5 - One Year Sustaining Membership - NonAutoRenewing Individual	Every 1 year (starting from join date)	$100.00 (USD)	No	Yes
Lifetime Business Membership Individual	Never	N/A	N/A	No
Lifetime Individual Membership Individual	Never	N/A	N/A	No

Membership Dues

The Board of Directors from time to time by resolution may change the annual dues that the membership is required to pay to the Corporation. Future annual dues shall be due and payable on the anniversary of the member's admission to membership. Membership shall be nontransferable and non-assignable.

Summary

Responsibilities

In the event of a violation of these policies and procedures, the Board or its designee will determine the proper response and/or action. Designees may include, but are not limited to any Executive Officer, Board Member, or Event Coordinator as the Board determines is appropriate.

5 CREDIT CARD SECURITY POLICY

(PCI DSS 3.0)

Introduction and Scope

Introduction

This document explains ABATE of Alaska, Inc.'s credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. ABATE of Alaska, Inc.'s management is committed to these security policies to protect information utilized by ABATE of Alaska, Inc. in attaining its business goals. All Board Members, Officers, Members, Contractors, and Volunteers are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, ABATE of Alaska, Inc.'s cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C-VT, ver. 3.0, released February, 2014. Should ABATE of Alaska, Inc. implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C-VT, it will be the responsibility of ABATE of Alaska, Inc. to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

All open ports and services must be documented. Documentation should include the port or service, source and destination, and a business justification for opening said port or service. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

Any mobile and/or Board Member, Officer, Contractor, and Volunteer-owned computers with direct connectivity the Internet (for example, laptops and phones used by Board Members, Officers, Members, Contractors, and

Volunteers), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or Board Member, Officer, Contractor, and Volunteer-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. ABATE of Alaska, Inc. must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse.
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.

- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable.

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) is not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

ABATE of Alaska, Inc. will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those Board Members, Officers, Contractors, Volunteers, and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, ABATE of Alaska, Inc. will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.). These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, ABATE of Alaska, Inc. will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability

ABATE of Alaska, Inc. will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to ABATE of Alaska, Inc.’s cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (also called “role-based access control). (PCI Requirement 7.1.3)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure All Areas and Media Containing Cardholder Data

Hard copy materials (media) containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, ABATE Membership Forms, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Requirement 12: Maintain a Policy that Addresses Information Security for Board Members, Officers, Volunteers, and Contractors

Security Policy

ABATE of Alaska, Inc. shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

Critical Technologies

ABATE of Alaska, Inc. shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)

Security Responsibilities

ABATE of Alaska, Inc.'s policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

The Board Chair shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Board Members, Officers, Members, Contractors, and Volunteers must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All Board Members, Officers, Members, Contractors, and Volunteers have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident

The current President and the Contract Bookkeeper should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the current President or the Contract Bookkeeper to report any suspected or actual incidents. The current President's or the Contract Bookkeeper's phone number should be well known to all Board Members, Officers, Members, Contractors, and Volunteers.

No one should communicate with anyone outside of their supervisor(s) or the current President or the Contract Bookkeeper about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the current President or the Contract Bookkeeper.

Document any information you know while waiting for the current President or the Contract Bookkeeper to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response Policy

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm
4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the current President and the Contract Bookkeeper will work with legal and management to identify appropriate forensic specialists.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Board of Directors and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

ABATE of Alaska, Inc. shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

ABATE of Alaska, Inc. shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI requirement 12.8.4)
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI requirement 12.8.5)

6 EVENT TRANSACTION POLICY

Introduction and Scope

Introduction

This document explains ABATE of Alaska, Inc.'s event transaction policy for volunteers that may represent ABATE of Alaska while assisting at event booths, trade shows, or other public functions. ABATE of Alaska, Inc.'s management is committed to these policies to protect the organization and information utilized by ABATE of Alaska, Inc. in attaining its business goals. All Board Members, Officers, Members, Contractors, and Volunteers are required to adhere to the policies described within this document.

Scope of Compliance

These event requirements apply to all Board Members, Officers, Members, Contractors, and Volunteers assisting with and participating in events representing ABATE of Alaska, Inc.

The requirements and procedures outlined below are intended to educate and protect ABATE of Alaska, Inc. and its volunteers who may be processing transactions or accepting donations on behalf of ABATE of Alaska, Inc.

Requirement 1: Events Kit

ABATE of Alaska "Events Kit"

ABATE of Alaska, Inc. maintains an "Events Kit" in a zippered case. Normally the Webmaster maintains possession of this kit to keep it updated and maintained. The "Events Kit" should be checked out by an approved responsible party who has signed the designated form acknowledging agreement with this Event Policy.

The contents of the "Events Kit" are owned by ABATE of Alaska, Inc. and are as follows:

1. Zippered Black Sleeve Pouch
2. Samsung Tablet with USB charging cord
3. Square-Up Magnetic Credit Card Reader
4. Square Reader for Contactless + Chip
5. Manilla Envelopes
6. Ledger
7. Ink Pens
8. Sharpie
9. Blank ABATE of Alaska, Inc. membership forms

Requirement 2: Transaction Ledger

Ledger

ALL transactions of any type for the day, without regard to method of payment, should be recorded in the ledger. Please use separate page(s) for each day. A copy of the page(s) should be made (can be photographed) and sent to the ABATE of Alaska, Inc. bookkeeper on a daily basis show all financial activity for that day at that event.

Methods of payment should be recorded in separate Columns:

- Cash
- Checks
- Credit Cards

The ledger should contain a full accounting of **ALL** transactions at any event. No ABATE of Alaska, Inc. transaction should occur that is NOT recorded in the ledger. Transactions should be listed in the order that they occur. Quantities and descriptions of each transaction (item, size, quantity, price, etc.) should be included for each transaction. Different items should be listed separately, even if paid for together.

Requirement 3: Processing Credit Cards

Tablet

The current ABATE of Alaska, Inc. tablet is a Samsung Galaxy Tablet. No logon is required to access the Register application on the main screen. All potential transactions should already be in the Register application.

The ABATE of Alaska, Inc. Webmaster maintains possession of the tablet to keep it updated and charged. Any ABATE of Alaska, Inc. Board Member, Officer, or Contractor may check it out to use at an event. ABATE of Alaska, Inc. Volunteers may also check it out if approved to represent ABATE of Alaska, Inc. at an event. Whoever checks out the device is responsible for keeping the device safe and in their possession and then returning the device within a reasonable agreed to time period following the event.

Square-Up Register App

The software is kept current. No login is required to process Credit Cards as a Guest. Internet Connectivity is necessary to process Credit Cards. All normally anticipated transactions are already included as items within the Register application.

Customers can have a receipt emailed to them through the application.

Square-Up Magnetic Credit Card Reader

The Square-Up Magnetic Credit Card Reader plugs into the earphone jack of the Samsung Tablet. The register app should detect it as soon as it is started.

Square-Up Reader for Contactless + Chip

The current Samsung Galaxy Tablet does not support the Bluetooth version required for the Square Reader for Contactless + Chip to work. Specific ABATE of Alaska, Inc. Board Members and Officers may have the Register application installed on a personal phone that can make use of this device as an individual one-off solution. Future tablet acquisitions by ABATE of Alaska, Inc. will need to ensure the inclusion of the appropriate Bluetooth version support.

Internet Access

Anyone who incurs a reasonable cost to provide Internet Access for the ABATE of Alaska, Inc. Tablet by setting up a Wi-Fi Hot Spot with their personal cell phone or paying a local Wi-Fi provider for daily Internet access is eligible for reimbursement. The expense must be submitted to the ABATE of Alaska, Inc. bookkeeper

Requirement 4: Memberships

Membership Forms

All transactions related to ABATE of Alaska, Inc. memberships should include a completed Membership Form. This includes New Memberships, Renewals, Membership changes, and Information Updates.

Membership transactions are also to be recorded in the ABATE of Alaska, Inc. ledger like any other transaction.

Membership Forms should accompany any cash or checks submitted or match up to applicable credit card transactions. These forms MUST include the following information:

1. Membership Type
2. First and Last Name
3. Current Phone Number
4. Current Email Address
5. Current Mailing Address
6. The prospective or renewing Members Signature
7. The method of payment
8. The amount received

If there is an issue with any of the above information, the phone number or email for the individual can be used to reach them for clarification.

Requirement 5: End of Each Day

Daily Event Audit

At the end of each day of an event, a picture or copy of the ledger should be sent to the current ABATE of Alaska, Inc. bookkeeper. Any cash and/or checks received along with any related paperwork should be put into individual envelopes as noted below.

Manilla Envelopes

The following transaction types, though listed together on the ledger, should be stored in separate manila envelopes labeled as follows if applicable:

Membership – Date - Event

Products – Date - Event

Donations – Date - Event

These envelopes should be delivered to the bookkeeper or dropped into the ABATE of Alaska, Inc. box at Alaska Leather on the first business following the event.

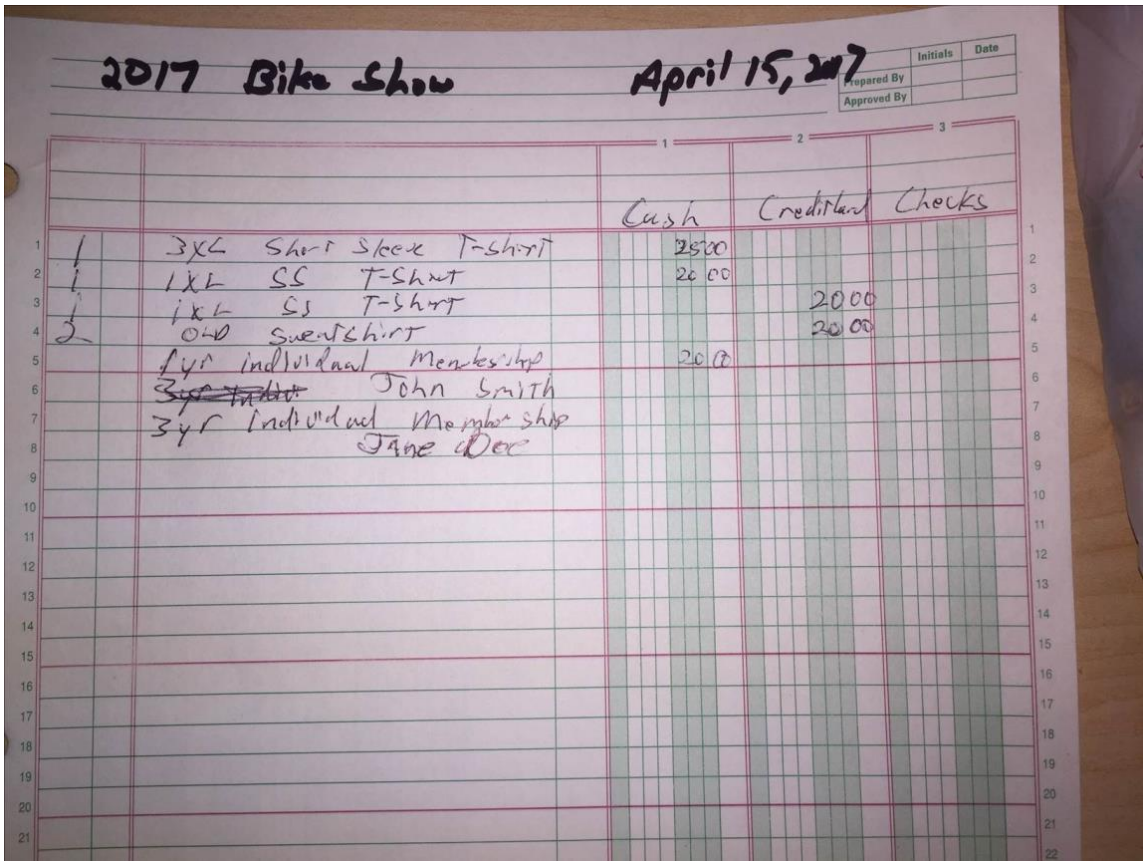
Summary

Responsibilities

Receipts for different ABATE of Alaska, Inc. transactions, different events, or different days should never be mixed. It is the responsibility of anyone working the event to make sure these processes are adhered to. Failure to do so endangers the ABATE of Alaska, Inc. organization and also increases the workload on the ABATE of Alaska, Inc. volunteers and the ABATE of Alaska, Inc. contract bookkeeper.

[redacted]Appendix 1

Sample Ledger (Please total each column at the bottom of the page.)



2017 Bike Show April 15, 2017

Prepared By	Initials	Date
Approved By		

			1 Cash	2 Credit Card	3 Checks
1		3XL Short Sleeve T-Shirt	25.00		
1		1XL SS T-Shirt	20.00		
1		1XL SS T-Shirt		20.00	
2		OLD Sweatshirt		20.00	
		1yr individual Membership	20.00		
		~~3yr Indiv~~ John Smith			
		3yr Individual Membership Jane Doe			