Information Security Policy ACST SAQ A

BEAVER DAM BAPTIST CHURCH

DATE: 08/15/2019

VERSION: 1

Introduction

This document defines the Beaver Dam Baptist Church security policy on the processing of card payments via the website (ecommerce, card-not-present) and handling of associated payment card data.

This security policy shall be reviewed annually and updated as needed and whenever the environment changes, to ensure policy statements remain appropriate for the protection of payment card data.

Scope

This policy applies to:

- All card-not-present Ecommerce (website) payments processed via the hosted payment page.
- All those parties with responsibility for managing and maintaining the Beaver Dam Baptist Church websites who must ensure that applicable policy requirements are implemented to help protect the websites from compromise and maintain the integrity of the redirection mechanism that links cardholders to the hosted web interface
- Managers/supervisors who must ensure that those staff understand their responsibilities and meet the requirements set out in this document.

Optionally, for churches that offer their church members and donors the ability to pay using Vanco Give+ Text or Give+ Mobile, this policy also applies to:

- All card-not-present (mobile) payments processed via the Vanco supplied and managed Give+ Text or Give+ Mobile solutions.

Definitions

- **Cardholder data** - includes the primary account number (PAN, the long card number shown on the payment card), cardholder name and expiry date.
- **Sensitive authentication data** - includes the full track data (magnetic stripe data or equivalent on the chip), card verification code or value (the three-digit or four-digit number printed on the card) and the PIN/PIN block.
- **Payment card** – defined by the PCI Security Standards Council[1] as any payment card bearing the logo of one of the PCI SSC's founding members: American Express, Discover, JCB, MasterCard or Visa.
- **Payment card data** – the cardholder data and sensitive authentication data shown on the card or stored in the magnetic stripe/chip).
- **Service provider** - Any third-party organisation which processes payment card data on behalf of Beaver Dam Baptist Church, that payment card data is shared with or that could impact the security of payment card data. For example, a document-retention business that stores paper documents that include payment card data.
- **SAQ - Self-Assessment Questionnaire** – the Church will self assess and attest to compliance with the PCI DSS.

[1] https://www.pcisecuritystandards.org/

- **Firewall** - Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
- **Systems** – in the context of this information security policy 'systems' refers to:
    - Any church web server that includes an Ecommerce redirection mechanism used to redirect the cardholder to a hosted web interface (hosted payment page) for submission of card payments
- **Administrator** –in the context of this information security policy 'administrator' refers to IT systems administrators, the internal or external personnel responsible for configuring, managing and maintaining computer systems, firewalls, network devices, web servers, etc.

Policy Statements

Approved payment method

All payment methods for the processing of payment card transactions must first be approved. Approval is provided by Katie Greene, Director of Finanance and Administration. Katie Greene, Director of Finance and Administration will maintain the list of approved payment methods.

The current credit card processing solution for the Church is provided by ACS Technologies. No other methods of card processing are permitted without prior approval of church leadership.

Website Ecommerce payments:

- Card payment submission and processing shall be via a hosted web interface (hosted payment page) accessed by the cardholder using an internet connected web browser
- All cardholder data functions must be entirely outsourced to PCI DSS validated third-party service providers
- All elements of the hosted payment page delivered to the cardholder's browser must originate only and directly from a PCI DSS validated third-party service provider
- Beaver Dam Baptist Church will not electronically store, process, or transmit any card data relating to Ecommerce payments on its own systems or premises, but will rely entirely on the third parties named above to handle all these functions
- Specifically, for online Ecommerce payments all processing and handling must satisfy the requirements set out in the SAQ A[2]

Optionally, churches may also offer their church members and donors the ability to pay using Vanco Give+ Text or Give+ Mobile.

Mobile payments:

- Card registration, payment submission and processing shall be via a hosted mobile web interface (hosted payment page) accessed from the member or donor's own mobile device
- All cardholder data functions must be entirely outsourced to the PCI DSS validated third-party service provider, Vanco Payment Solutions
- All elements of the hosted mobile card registration and payment page delivered to the cardholder's mobile device must originate only and directly from a PCI DSS validated third-party service provider

[2] As of May 2018: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A-rev1_1.pdf

- Beaver Dam Baptist Church will not electronically store, process, or transmit any card data relating to Mobile payments on its own systems or premises, but will rely entirely on the third party named above to handle all these functions
- Specifically, for Vanco Give+ Text or Give+ Mobile payments all processing and handling must satisfy the requirements set out in the SAQ A[3]

No other receipt or transmission of payment card data via electronic means is permitted.

The approved payment methods used ensure that payment card data is properly encrypted, using industry-standard strong cryptography and security protocols, when it is sent (transmitted) over the Internet.

Configure Systems Securely

Default / factory settings, default usernames or account names and passwords that come with or are pre-set on systems must be changed or disabled before the systems are installed. In addition, any unnecessary default accounts, must be disabled or removed from systems.

Protect payment card data

Any paper documents showing cardholder data must be held securely. This includes physically securing media to prevent it being accessed or viewed by personnel with no church/business need to see payment card data.

Methods to physically securing paper documents may include storing them in a locked drawer, cabinet or safe, or other method that protects the media from unauthorized access, accidental loss or theft.

Cardholder data must not be retained electronically.

Cardholder data must be securely destroyed, or redacted to obscure or 'black out' the cardholder data, when it is no longer needed for a business reason.

Approved methods of destruction of payment card data include cross cut shredded, incinerated or pulped so that cardholder data cannot be reconstructed.

If payment card data is placed into storage containers prior to destruction, e.g. by a third-party document destruction company, those containers must be secured to prevent access to the contents.

The movement or distribution of any media containing or showing payment card data must be controlled, for example when transferring chargeback letters from the mail room to administrative offices:

- Identify and classify any such media (i.e. as 'confidential') to ensure appropriate handling by staff, volunteers, etc.
- If any media containing payment card data is sent/moved between church locations, it must always be sent by a secure and tracked method or kept 'in hand' by church staff

Make sure that there is church management approval for any such movement or distribution of media containing payment card data, i.e. approval of method used, signatory on courier tracking receipt.

[3] As of May 2018: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A-rev1_1.pdf

Implement Strong Access Control Measures to keep access to a minimum

Separate administrator and user logins (accounts) must be used, so that administrative rights can be given only to delegated personnel who need the extra level of access and rights to be able to do their job. For example, web server administrators.

All systems users/administrators must have their own individual login (unique id) and password. This includes any users/administrators with access to a church web server that is set-up with an ecommerce redirection mechanism, this is to help protect the website/web server from compromise and maintain the integrity of the redirection mechanism.

Systems must require the selection of strong passwords, which must be of a minimum of seven alphanumeric characters.

A token device, smart card or biometric may be used instead of passwords to authenticate systems users and administrators.

Use of generic usernames, accounts or shared user ID's (shared accounts), including shared passwords, is not permitted.

Access to systems must be removed for personnel on the termination of their relationship with the church, their employment or contract.

Service Providers

A current and accurate list of approved service providers must be maintained including contact details and a description of the services provided. The list must include third party service providers that payment card data is shared with or that could impact the security of payment card data. This includes any third-party delivered service that may:

- Affect processing of card payments via the hosted web interface payment channel,
- Affect the handling, or protection of payment card data,
- Affect processing of card payments via Vanco Give+ Text or Give+ Mobile payment channels (if available to Beaver Dam Baptist Church members and donors)

There must be a written agreement with each service provider that includes an acknowledgement by the service provider of their responsibility for securing the payment card data they possess, process or transmit on Beaver Dam Baptist Church’s behalf.

Due diligence must be exercised before engaging with any service providers that may affect Beaver Dam Baptist Church’s cardholder data environment, card payment processing or handling of payment card data. For example, when engaging a third-party data destruction company, perform checks necessary to verify the potential supplier's ability to fulfil their PCI DSS responsibilities.

For Beaver Dam Baptist Church’s use of the Approved payment methods to remain eligible for the PCI DSS SAQ A, the service providers ACS Technologies and Vanco Payment Solutions must maintain their status as validated PCI DSS compliant service providers.

Service providers’ compliance with PCI DSS will be monitored and checked at least annually.

Any agreement with a service provider must make clear which PCI DSS requirements are to be managed by the service provider, and which will be the responsibility of Beaver Dam Baptist Church.

Security Incident Response

A security incident response and escalation procedure must be created. See Appendix C.

Appendix A:

Agreement to Comply with Information Security Policies

This Information Security Policy has been approved by Beaver Dam Baptist Church, Finance Committee to ensure that all payment card data is protected and used in the best interests of the Church and its congregants.

It is important that we all understand the importance of protecting payment card, our responsibilities and the consequences of ignoring them.

It is important that you recognize and understand your role in protecting payment card data. The Information Security Policy will help you understand your role in this important aspect of our business's activities. Please read this Policy and all associated policies and procedures.

If there is anything you do not understand, please speak to manager/administrator who will be able to advise you.

Declaration

Katie Greene
Staff/Employee Name (printed)

August 15, 2019
Date

I agree to take all reasonable precautions to assure that payment card data that has been entrusted to Beaver Dam Baptist Church by third parties such as congregants will be protected in accordance with these policies and shall not be disclosed to unauthorized persons.

I have access to a copy of the Information Security Policy, I have read and understand the policy statements, and I understand how the Policy impacts the function I am fulfilling. As a condition of continued employment/volunteering, I agree to abide by the policies and other requirements found in associated policies and procedures. I understand that non-compliance will be cause for disciplinary action up to and including dismissal (for volunteers: revocation of my volunteer status).

I also agree to promptly report all violations or suspected violations of information security policies to the nominated individual(s)

Katie Greene
Employee Signature

Appendix B:

The solutions used in our Church are:

- Realm
- Vanco Give+ Text
- Vanco Give+ Mobile

Appendix C: Security Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled or coerced employee or congregant, and their intention might be to steal information, cardholder data, or just to damage your Church.

The Incident response plan must be tested at least annually. Copies of the incident response plan are to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees and volunteers of the Church will be expected to report to the nominated individual(s) for any security related issues. The nominated individual(s) may be a member of the PCI Response Team, the Management team or individual(s) who have been trained to respond to incidents.

The Church PCI Security Incident Response Plan is a separate document from this security policy and can be found [insert location].

Download a template here: https://sysnetgs.com/wp-content/uploads/2017/11/Security-Incident-Response-Plan-1.dotx

Complete as necessary and edit this document with its location, removing the link above.

The Procedure for a security incident is as follows:

1. Church staff and volunteers must report incidents and suspected breaches to the nominated individual(s)
2. That member of the team receiving the report will advise the management team of the incident, if applicable.
3. The nominated individual(s) will investigate the incident utilizing the Security Incident Response Plan and assist in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The nominated individual(s) will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The nominated individual(s) will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
6. A Church that reasonably believes it may have had an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform the Church nominated individual(s). After being notified of a compromise, the nominated individual(s), along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

The Church nominated individual(s) is/are: **(Update as applicable)**

The card companies have individually specific requirements the nominated individual(s) must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications and reporting requirements to various card schemes can be found in the Security Incident Response Plan.

Appendix D: List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date