Vestry Approved October 19, 2020

Information Security Policy

St. Martha's Episcopal Church

Vestry Approved October 19, 2020

Contents

Vestry Approved October 19, 2020

Introduction

This Policy document applies to St. Martha's Episcopal Church (hereinafter the "Church") and encompasses all aspects of security surrounding confidential information. This Policy must be distributed to all Church employees. All Church employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by the Vestry of St. Martha's Episcopal Church whenever relevant, to include newly developed security standards into the policy, and re-distributed to all employees and contractors where applicable.

Definitions

Cardholder Data: All the following elements constitute cardholder data:

At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following:

Cardholder name
Expiration date and/or
Service code (found on the magnetic stripe)

PAN – Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Service Code – Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various purposes, such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Magnetic Stripe Data – Also referred to as "full track data" or "track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. This can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

Sensitive Authentication Data – Security-related information (including but not limited to card validation codes/values, full tract data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Card Verification Code – Also known as Card Validation Code or Value, or Card Security Code. The three digit or four digit value printed on the front or back of a payment card (CVV2 and CVC2 data). This refers to either: (1) magnetic-stripe data, or (2) printed security features.

PIN – Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN they provide matches the PIN in the system. Typical PINs are used for automated teller machines (ATMs) for cash advance transactions. Another type of PIN is one used in the EMV chip cards where the PIN replaces the cardholder's signature.

Point of Sale (POS): Hardware and/or software used to process payment card transactions at merchant locations.

Payment Card: Any payment card, including debit cards, which is issued by one of the leading payment card brands or associations.

Information Security Officer – Appointed by the Vestry, this person acts as the focal point for information security and serves as chairperson of the Church PCI Security Incident Response Team (PCI Response Team).

Information Security Policy

It is the policy of St. Martha's Episcopal Church that no one among the Clergy, employees, and officers of St. Martha's Episcopal Church, and members acting on behalf of St. Martha's Episcopal Church, is authorized to receive, collect, handle or transmit cardholder data belonging to any member of the church or the public in any manner whatsoever.

St. Martha's Episcopal Church accepts payment card donations solely through the Church website. None of the cardholder data processed through the website is available to Clergy, employees, or officers of St. Martha's Episcopal Church, or to members acting on behalf of St. Martha's Episcopal Church.

The Clergy, Administrative Assistant, Senior Warden, Treasurer and Assistant Treasurer are authorized to use the debit cards associated with the Church accounts at PNC Bank. As such, these persons have access to the cardholder data associated with the debit cards related to the Church accounts at PNC Bank.

St. Martha's Episcopal Church does not (as of the date of this Information Security Policy) own, lease or otherwise have access to point of sale devices or software. If at any time in the future the Church acquires or gains access to point of sale devices or software, this Information Security Policy will need to be updated to include safeguarding cardholder information handled in such manner.

St. Martha's Episcopal Church handles sensitive cardholder information in regard to the aforementioned debit cards on the Church's PNC accounts. Sensitive Information must have

adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organization.

Employees of the Church and members acting on behalf of the Church who handle sensitive cardholder information should:

- Handle Church cardholder information in a manner that fits with their sensitivity and classification;
- Limit personal use of the Church information and telecommunication systems;
- Not use e-mail, internet and other Church resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Not disclose personnel information unless authorized;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Not install unauthorized software or hardware, including modems and wireless access, unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Report information security incidents without delay to the Information Security Officer.

The Church reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose. Each Church employee, officer and member acting on behalf of the Church has a responsibility for ensuring our Church's systems and data are protected from unauthorized access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the Chairperson of the Technology Committee and the Information Security Officer.

Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The current version of the network diagram is attached at Appendix D. The network diagram provides a high level overview of the information environment.

Vestry Approved October 19, 2020

Acceptable Use Policy

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the Church's established culture of openness, trust and integrity. The Church is committed to protecting the employees, officers, parishioners and the Church from illegal or damaging actions, either knowingly or unknowingly by individuals. The Church will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

All Clergy, employees, officers and persons acting on behalf of the Church:

- Are responsible for exercising good judgment regarding the reasonableness of personal use.

- Should take all necessary steps to prevent unauthorized access to confidential data which includes cardholder data.

- Are directed to keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. All PCs, laptops and workstations should be secured with a password-protected screensaver.

The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. An inventory of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices. Users should identify any behavior which they believe indicates tampering or substitution. Any suspicious behavior will be reported accordingly. Information contained on portable computers is especially vulnerable, special care should be exercised.

Postings by employees from a Church email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Church, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan-horse code.

Protect Stored Data

All sensitive cardholder data handled by the Clergy, employees, officers and persons acting on behalf of the Church must be securely protected against unauthorized use at all times. Any sensitive cardholder data that is no longer required for business reasons must be discarded in a secure and irrecoverable manner. If there is no specific need to see the full PAN (Permanent Account Number) of the debit cards associated with Church PNC accounts, it has to be masked when displayed.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.

2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.

3. The PIN or the encrypted PIN Block under any circumstance.

Information Classification

Data and media containing information and/or data must always be labelled to indicate sensitivity level.

Confidential data might include information and/or data for which there are legal requirements preventing disclosure or financial penalties for disclosure, or information or data that would cause severe damage to the Church if disclosed or modified. Confidential data includes cardholder data.

Internal Use data might include information and/or data that the owner feels should be protected to prevent unauthorized disclosure.

Public information and/or data is such as may be freely disseminated.

Access to Sensitive Cardholder Data

All access to sensitive cardholder information associated with the Church debit cards related to the PNC accounts should be controlled and authorized. Any job functions that require access to cardholder data should be clearly defined.

Any display of the cardholder data should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.

Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to the Clergy, Administrative Assistant, Senior Warden, Treasurer and Assistant Treasurer.

If Church cardholder data associated with the debit cards on Church PNC accounts is shared with a Service Provider (3rd party), a record of the transaction will be maintained.

The Church will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.

Physical Security

Access to sensitive cardholder information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive cardholder information.

Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc. Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.

"Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration.

Strict control is maintained over the external or internal distribution of any media containing cardholder data and has to be approved by management

Strict control is maintained over the storage and accessibility of media

All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorized use.

Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically. Cardholder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into Church practice to maintain a high level of security awareness.

Handling procedures for sensitive information and security awareness will be addressed at Technology Committee meetings, and findings will be incorporated procedures into day to day Church practice.

It is required that all employees confirm that they understand the content of this Information Security Policy document by signing an acknowledgement form (see Appendix A).

Church information security policies must be reviewed annually and updated as needed.

Vestry Approved October 19, 2020

Credit Card (PCI) Security Incident Response Plan

The Church PCI Security Incident Response Team (PCI Response Team) is led by the Information Security Officer and comprised of the Technology Committee and PNC Merchant Services. The Church PCI security incident response plan is as follows:

1. An incident must be reported to the Information Security Officer or to another member of the PCI Response Team.

2. That member of the team receiving the report will advise all other members of the PCI Response Team of the incident.

3. The PCI Response Team will investigate the incident and assist in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.

4. The PCI Response Team 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 PCI Response Team 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.

The Church PCI Security Incident Response Team:

The Information Security Officer
All members of the Technology Committee
Senior Warden
Rector

Information Church PCI Security Incident Response Procedures:

Any Church employee or member acting on behalf of the Church who reasonably believes an account breach has occurred (or a breach of cardholder information, or of systems related to the PCI environment in general) must inform the Church PCI Incident Response Team. After being notified of a compromise, the PCI Response Team will implement the PCI Incident Response Plan.

Incident Response Notification. The Information Security Officer will take the lead to notify:

External Contacts (as needed)
Merchant Card Provider
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable) Communication Carriers (local and long distance)
Insurance Carrier

Law Enforcement Agencies (as applicable in local jurisdiction)

In response to a systems compromise, the PCI Response Team will:

1. Ensure each compromised system is isolated on/from the network.
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the PCI Security Incident Response Team must address in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

1. Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.

2. Alert all affected parties and authorities such as the Merchant Bank (PNC Bank), Visa Fraud Control, and the law enforcement.

3. Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.

4. For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as “VISA Secret”*

Vestry Approved October 19, 2020

I. Executive Summary

a. Include overview of the incident
b. Include RISK Level (High, Medium, Low)
c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures - Include forensic tools used during investigation

V. Findings

a. Number of accounts at risk, identify those stores and compromised
b. Type of account information at risk
c. Identify ALL systems analyzed. Include the following:
   - Domain Name System (DNS) names
   - Internet Protocol (IP) addresses
   - Operating System (OS) version
   - Function of system(s)
d. Identify ALL compromised systems. Include the following:
   - DNS names
   - IP addresses
   - OS version
   - Function of System(s)
e. Timeframe of compromise
f. Any data exported by intruder
g. Establish how and source of compromise
h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.

II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to:
compromised_account_team@mastercard.com.

III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.

IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).

V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.

VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.

VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of the Church will be expected to report to the Information Security Officer for any security related issues. The role of the Information Security Officer is to effectively communicate all security policies and procedures to employees within the Church and contractors. In addition to this, the Information Security Officer will monitor and enforce the security policies outlined in this document and oversee the implementation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102

II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances

III. Prepare a list of all known compromised account numbers

IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.

II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances

III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Transfer of Sensitive Information Policy

All third-party companies providing critical services to the Church must provide an agreed Service Level Agreement. All third-party companies providing hosting facilities must comply with the Church's Physical Security and Access Control Policy.

All third-party companies which have access to cardholder information must:

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the cardholder data.
3. Acknowledge that the cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

Vestry Approved October 19, 2020

User Access Management

Access to the Church network is controlled through a user registration process. Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out. Access to all the Church systems is provided by the Chairperson of the Technology Committee and can only be started after proper procedures are completed. As soon as an individual leaves the Church employment, all his/her system logons must be immediately revoked. As part of the employee out-processing, the Senior Warden will inform the Chair of the Technology Committee of all leavers and their date of leaving.

Access Control Policy

Access Control systems are in place to protect the interests of all users of the Church computer systems by providing a safe, secure and readily accessible environment in which to work.
The Church will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled.

Access rights will be accorded following the principles of least privilege and need to know.

Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.

Users are obligated to report instances of non-compliance to the Information Security Officer.

Access to the Church IT resources and services will be given through the provision of a unique account and complex password.

No access to any the Church IT resources and services will be provided without prior authentication and authorization of a user's need for access.

Access to Confidential, Restricted and Protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

Users are expected to become familiar with and abide by the Church policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.

Access for remote users shall be subject to authorization by the Chairperson of the Technology Committee and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.

A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with the Technology Committee to review users' access rights.

Vestry Approved October 19, 2020

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

_____
Employee Name (printed)

_____
Department

I agree to take all reasonable precautions to assure that Church internal information, or information that has been entrusted to the Church by third parties such as parishioners, members of the public customers, or service providers will not be disclosed to unauthorized persons. At the end of my employment or contract with the Church, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive 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 manager who is the designated information owner.

I have access to a copy of the Information Security Policy document, I have read and understand this policy, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Church Information Security Policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Information Security Officer.

_____
Employee Signature

_____
Date

Vestry Approved October 19, 2020

Appendix B – List of Devices

Device Name	Description	Approved User	Location
Cisco DPC3008	Internet Modem	Network Subscribers	Closet outside Parish Hall
Arris TM804	Mediacom telephone switch	Parish telephone	Closet outside Parish Hall
Netgear WNR3500L v2	Router	Network Subscribers	Closet outside Parish Hall
Dell Power Connect 2716	16 Gigabit Port Switch	Network Subscribers	Closet outside Parish Hall
Wireless dimming system	Caserta	Parish Hall users	Closet outside Parish Hall
Copier	Sharp MS-3050 Network Copier	Network Subscribers	Parish office
Laptop Computer	Dell Alienware	Administrative Assistant	Parish office
Laptop Computer	Dell Inspiron 17	Director of Music	Director's Office
Laptop Computer	Apple MAC	Interim Priest	Rector's Office
Laptop Computer	Dell	Deposit Coordinators	Sacristy
Dual Band Wireless System	TP-Link Deco MS AC1300	Network Subscribers	3 Units: 1 in Closet outside Parish Hall 1 in Parish Hall 1 in Sanctuary

Appendix C - List of Service Providers

Name of serviced Provider	**Service Provided**
Mediacom	Internet service provider
Dream Host	Website Hosting
PNC Bank	Merchant Bank
PNC Business Track	Credit Card Payment Log
Payeezy	Payment Card Processing
Clover Security	Payment Card Industry Date Security Standard (PCI DSS) Compliance

Mediacom = URL

PNC Bank = www.pnc.com

PNC Business Track = https://www.myclientline.net/welcome.html

Payeezy = https://globalgatewaye4.firstdata.com/?lang=en

Clover Security = https://pnc.cloversecurity.com/safemaker/login/login-portal

Appendix D – Network Diagram