Information Security Policy

United Church of Christ, Congregational, of Boxborough

Effective Date: Final, 12 January 2017

Supercedes Date: n/a

1 Purpose

This Policy describes the handling and security of confidential information stored on electronic devices operated by the church and applies to all church employees or volunteers who utilize these devices.

The United Church of Christ Congregational, Boxborough (the Church) utilizes a credit card reader to collect payment at certain events. This policy will ensure that there are adequate safeguards in place to protect cardholder data, cardholder privacy, and to ensure compliance with Payment Card Industry Data Security Standard (PCI DSS) in addition to protecting the Church, it's employees, and volunteers from liability.

2 Definitions

The United Church of Christ, Congregational, of Boxborough is referred to as the *Church* in this Policy.

PCI DSS stands for Payment Card Industry Data Security Standard.

POS stands for Point of Sale device (ie, credit/debit card reader).

3 Procedures

3.1 Administration

All employees and volunteers engaged in utilization of church owned electronic devices and systems will read this Policy.

This Policy will be reviewed by the church Finance Team on an annual basis or when relevant to include newly developed security standards into the Policy. Following revision, the Policy will be redistributed to the appropriate employees and volunteers for training purposes.

3.2 Protect Privacy

The Church commits to respecting the privacy of its employees, volunteers, members and friends. To this end, the Church is committed to maintaining a secure environment on all electronic devices and systems that process sensitive information, including financial transactions. Employees and volunteers handling sensitive information on Church electronic systems will ensure the following:

- Records containing sensitive information and financial transactions shall be handled in a confidential manner befitting the nature of the information or record.
- Use of Church information is limited to strictly Church business. Electronic systems provided by the church should be used for Church business, providing for limited personal use of the internet and WIFI.
- Understand that Church systems may be audited or monitored at any time for appropriate use.
- Church systems will not be used to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Electronic device usernames, passwords, and account information will be kept confidential.
- Software or hardware will not be installed on Church systems without prior discussion with the Finance Team, or Church Administrative Assistant.
- Incidents that may compromise sensitive records, information, or systems are reported immediately to the Church Treasurer, Administrative Assistant, Moderator and/or Pastor.

3.3 Network Security

The Church maintains a desktop computer system for the Church Administrative Assistant and ministry team use and a POS device for receiving credit/debit card payment. To assist with maintaining information security the Church should ensure the following:

- All electronic systems should be maintained with industry standard security software.
- Computer hardware, point of sale (POS) devices, and PIN entry devices should be kept in a secure location when not in use.

- Employees and volunteers should use extreme caution when opening email attachments or web links received from unknown senders, which may contain computer viruses or malware.

- Church email accounts should be used for church business and not personal communication.

3.4 Protect Stored Data

All sensitive financial data, including payment card or banking information handled by the Church and its employees or volunteers must be protected against unauthorized use at all times. Any sensitive data that is no longer required by the Church for business reasons must be discarded in a secure and irrecoverable manner.

When utilizing the payment card reader 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.

3.5 Information Classification

Data and media containing sensitive datashould be labeled appropriately.

- Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the Church if disclosed or modified. Confidential data includes payment cardholder data, financial donations, pledge payments, etc.

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

- Public data is information that may be freely disseminated.

3.6 Access to the Sensitive Cardholder Data

All access to sensitive payment card data should be controlled and authorized.

- Any display of payment card information should be restricted to 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 employees that have a legitimate need to view such information.

- No other church employees or volunteers should have access to this confidential data unless they have a genuine business need.

- If cardholder data is shared with a Service Provider (3rd party) then a list of these Service Providers should be maintained with the Church Administrator.

- The Church will ensure that there is proper due diligence in place, before engaging with any Service provider that may obtain or have access to financial or other confidential information.

3.7 Physical Security

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

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, USB drives, back-up tapes, computer hard drives, etc.

- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.

- Point of Sale (POS) devices should be stored in a secure area when not in use.

- Individuals using POS devices should be trained on their use and receive instructions regarding secure handling of the device.

- Any evidence of tampering or unauthorized information access in regards to the Church electronic systems or POS device must be immediately reported to the Church Treasurer, Administrative Assistant, Moderator and/or Pastor.

3.8 Protect Data in Transit

All sensitive data or information must be protected securely if it is to be transported physically or electronically.

Credit cardholder data must never be sent over the internet via e-mail, instant chat or via other end user technologies. If there is a business need to transmit cardholder data then it must be done using a strong encryption mechanism. Only secure courier services should be used for transporting or mailing sensitive cardholder data to another location, and all such transactions will be monitored or tracked to ensure the information reaches its intended location.

3.9 Disposal of Stored Data

All financial or other sensitive information no longer required by the Church must be disposed of in a secure manner. Hardcopy materials should be shredded, incinerated or pulped so they cannot be reconstructed. Information stored on electronic media will be permanently deleted and rendered unrecoverable.

The Church will periodically conduct reviews of financial information to evaluate the need for retention.

3.10 Security Awareness and Procedures

This security policy should be distributed to all new Church employees or volunteers who may have the opportunity to handle sensitive information. The policy should be reviewed by all affected individuals on an annual basis.

Church employees that handle sensitive information will undergo background checks within the limits of local law before they commence their employment with the Church.

All third party companies providing critical services to the Church that may have access to sensitive data should be monitored and provide a service level agreement. Providers that may have access to credit card holder information are contractually obligated to comply with card associate security standards (PCI/DSS).

3.11 Security Incident Response Plan

Any known or suspected breach of data security will be reported immediately to the Church Treasurer, Administrative Assistant, Moderator and/or Pastor. Notifications must occur at minimum within 24 hours of the event. The person receiving notification will work with the other responsible individuals to investigate the incident, take action to limit additional negative exposure, and report the incident to the appropriate authorities or parties (credit card companies, local law enforcement, internet service providers, card holders, etc.) as necessary.

Compromised systems, POS devices, or processes involved in the breach should be shut down to limit the extent of the problem and prevent further exposure.

Credit card companies have individually specific reporting requirements that must be met to address any suspected or confirmed breach of cardholder data. All compromised credit card accounts must be reported to the issued card service within 24 hours of the incident and the prescribed reporting process must be followed and documented.

Following incident resolution the Treasurer, Administrative Assistant, Moderator and Pastor should evaluate the need for updating of policies, training, or security in order to avoid future incidents.

3.12 Acceptable Use Policy

Employees and volunteers utilizing the electronic devices and systems of the Church are responsible for exercising good judgment regarding the use of the devices and take all necessary steps to prevent unauthorized access to confidential data.

3.13 Amendments to the Policy

This policy can be amended for administrative changes by any member of the Finance Team. Review of the policy should be conducted by the Finance Team on an annual basis and be updated as needed.

4 Forms

Not applicable.