Information Security Policy

Cedar Park First United Methodist Church

Revision 2 - Approved, 27 June 2022 - Updated for latest PCI-DSS requirements
Revision 1 - Updated 27 December 2020 - List of Devices, p.9

Originally Approved for Use 17 September 2018

Contents

Introduction

This Policy document encompasses all aspects of security surrounding confidential church information and must be distributed to all church employees and authorized personnel using the church Information Technology (IT) infrastructure. All church employees and authorized personnel using the church IT infrastructure must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document may be reviewed and updated by church leadership on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and authorized personnel where applicable.

Information Security Policy

Cedar Park First United Methodist Church (CPFUMC) commits to respecting the privacy of all its authorized personnel and to protecting any member data from outside parties. To this end church leadership are committed to maintaining a secure environment.

- Limit personal use of CPFUMC information and telecommunication systems and ensure it doesn't interfere with your job performance;
- CPFUMC reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, Internet, Local Area network (LAN) and other church resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose member or employee information unless authorized;
- Keep passwords and accounts secure;
- Request approval from the CPFUMC LAN Administrator prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorized software or hardware, including modems and wireless access points unless you have explicit LAN Administrator approval;
- Always leave desks clear of sensitive data and log out from computer screens when unattended;
- Information security incidents must be reported, without delay, to the Pastor and LAN Administrator.

We each have a responsibility for ensuring our church 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 Pastor or LAN Administrator.

1. Network Security

A high-level network diagrams of the CPFUMC network (1, 2) are maintained and reviewed on a yearly basis. The network diagrams provide a high-level logical overview of the wiring, connections and components in the CPFUMC Local Area Network (LAN).

- The access passwords for all routers and wireless access points are changed from the vendor-supplied defaults.
- Any unnecessary computer login accounts are removed when no longer needed.
- All computer systems, routers and wireless access points are maintained with up-to-date firmware and security patches installed within one month of release.

2. Acceptable Use Policy

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

- Employees and authorized personnel are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees and authorized personnel should take all necessary steps to prevent unauthorized access to confidential data
- Keep passwords secure and do not share accounts. Employees and authorized personnel are responsible for the security of their passwords and accounts.
- The List of Managed Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.
- Users should be trained in the ability to identify any suspicious behavior where any tampering or substitution may be performed. 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 (xxxxxx@cpfumc.org) to newsgroups are not allowed.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3. Information Classification

Data and media containing data must always be labeled to indicate sensitivity level.

1. **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 CPFUMC if disclosed or modified.
2. **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure. This includes some of our shared Google docs.
3. **Public data** is information that may be freely disseminated. This includes some of our shared Google docs.

4. Access to the Sensitive Cardholder Data

The church will ensure that there is an established process, including proper due diligence is in place, before engaging with a credit card Service provider (such as Vanco, PayPal or Regions Bank). The church will have a process in place to monitor the Payment Card Industry Data Security Standard (PCI-DSS) compliance status of the Service provider (Vanco). The current policy of the church is that all credit card transactions related to the church are settled on third party systems which comply with PCI-DSS (such as Vanco and Region's Bank) and not on any church IT systems.

5. Physical Security

Access to sensitive information in both hard and 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, backup tapes, computer hard drives, flash drives, etc.
- Media containing sensitive 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 information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, authorized personnel, volunteers and consultants who are on the church site. 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, usually not more than one day.
- Strict control is maintained over the storage and accessibility of media.

6. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the CPFUMC Records Retention Policy, regardless of the media or application type on which it is stored.
- All hard copies of data must be manually destroyed (shredded) when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- CPFUMC will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are shredded, incinerated or pulped so they cannot be reconstructed.
- CPFUMC will have documented procedures for the destruction of electronic media. These will require:
  - All data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
  - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.
- The life cycle of financial hardcopy records and other hardcopy and electronic records is managed in accordance with the Cedar Park First United Methodist Church Records Retention Policy and Schedule.

7. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into church practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees, volunteers and authorized personnel.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day practice.
- Distribute this security policy document to all church employees, volunteers and authorized personnel to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with CPFUMC.
- CPFUMC security policies must be reviewed annually and updated as needed.

8. Security Incident Response Plan

Any data security incidents will be reported immediately to the Pastor for the appropriate response.

9. 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 which have access to Cardholder information must
    1. Adhere to the PCI DSS security requirements and acknowledge their responsibility for securing the Cardholder data.
    2. Acknowledge that the Card Holder 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.
    3. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
    4. 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.

10. User Access Management

- Access to church information technology systems is controlled through a formal user registration process beginning with a formal notification from the SPRC for new employees and for the Pastor or committee chairperson for other volunteers and authorized users.
- Each user is identified by a unique user ID and password so that users can be linked to and made responsible for their actions. The use of group IDs or shared IDs is not permitted.
- There is a standard level of access; other services can be accessed when specifically authorized by the Pastor.
- The job function of the user decides the level of access the employee or volunteer has to data.
- A request for service must be made in writing (email or hard copy) by the Pastor or committee chairperson. The request is free format, but must state:

    1. Name of person making request;
    2. Job title of the employee;
    3. Start date;
    4. Services required (default services are: PC Login account and Internet access)

- Access to all CPFUMC systems is provided by the LAN Administrator and can only be started after proper procedures are completed.
- As soon as an individual leaves CPFUMC employment or their volunteer position, all his/her system logons must be immediately revoked.

- As part of the employee termination process the Pastor or SPRC chair will inform the CPFUMC LAN Administrator of all leavers and their date of leaving.

11. Access Control Policy

- Access Control systems are in place to protect the interests of all users of CPFUMC computer systems by providing a safe, secure and readily accessible environment in which to work.
- CPFUMC will provide all employees and other authorized personnel with the information they need to carry out their responsibilities in an effective and efficient manner as possible.
- Group IDs are not permitted.
- The allocation of privilege rights (e.g. local administrator, , super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and LAN Administrator.
- 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 Pastor.
- Access to CPFUMC IT resources and services will be given through the provision of a unique login account and password.
- Each password will be a combination of at least 7 letters, numbers and characters.
- No access to any CPFUMC IT resources and services will be provided without prior authentication and authorization of a user's user id and password.
- Password issuing, strength requirements, changing and control will be managed through formal processes by the LAN Administrator. Password length, complexity and expiration times will be controlled.
- 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.
- Users are expected to become familiar with and abide by CPFUMC 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 CPFUMC LAN Administrator.
- Access to data is variously and appropriately controlled according to the data classification levels.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, firewall permissions, SQL database rights, and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with the LAN Administrator to review users' access rights. The review shall be logged and the LAN Administrator shall authorize users' continued access rights.

Appendix A – Agreement to Comply with Information Security Policies

____

Employee/Volunteer Name (printed)

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 authorized personnel, will not be disclosed to unauthorized persons. At the end of my volunteer time or 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 Pastor.

I have access to a copy of the Information Security Policy, I have read and understand this policy, and I understand how it impacts my job. As a condition of continued employment or volunteering, I agree to abide by the policies and other requirements found in the 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 Pastor.

____

Employee/Volunteer Signature

____

Date

Appendix B – List of Managed Devices**

Asset/Device Name	Description	Owner/Approved User	Location*
Router/Gateway	Arris DFG-1670A	Spectrum/ CPFUMC LAN Admin	MMB Utility Closet
Router	Netgear R6300v2	CPFUMC LAN Admin	MMB Utility Closet
Routers (WAPs)	Netgear Nighthawk AC1900 (R7000) TP-Link AC1900 Archer C9 TP-Link AC1750 Archer A7	CPFUMC LAN Admin	Sanctuary Nursery (in Sanct. Blg.) MMB Classroom 4
Printer/Copier/Scanner	Sharp model MX-3071	Sharp USA/Authorized employees; authorized church personnel	Church office
Printer	Kyocera model M2635dw	Authorized employees; authorized church personnel	Suzette's office
Computers	Various Dell OptiPlexes, Dell Vostro and Latitude laptops	Authorized employees; authorized church personnel (volunteers)	Sanctuary Building (7) Multi-Ministries Building (7)
NAS (2)	Buffalo Linkstation LS-210D	CPFUMC LAN Admin	Sound Booth and MMB Utility Room
Unmanaged Network Switches (6)	Various (6) Netgear and TP-Link 5- and 8-port models	CPFUMC LAN Admin	Sanctuary Building (3) Multi-Ministries Building (3)
Managed Network Switches (3)	2 x Netgear GC110P 1x TP-Link TL-SG108PE	CPFUMC LAN Admin	Multi-Ministries Building (1) Sanctuary Building (2)
Managed Wi-Fi Irrigation Controller (1)	Hunter model HCC-800-PL	Trustees	N. Exterior of Sanctuary Building

Managed Wi-Fi Thermostats (8)	Honeywell model TH8321WF1001	Trustees	4 in Sanctuary Building 4 in MMB
Managed Telephone Base Stations (2)	Ooma Office Base Station	CPFUMC LAN Admin	MMB Utility closet
Ring Video Doorbell (1)	Ring Doorbell 3	CPFUMC LAN Admin	MMB front door
Ring Chimes (2)	Ring	CPFUMC LAN Admin	Church Office, Hallway
ATEM Mini video switch (1)	Black Magic Designs	Live Streaming Team	Sanctuary
PTZ camera (1)	PTZ Optics model PT20x-NDI-WH	Live Streaming Team	Sanctuary

*See the Cedar Park First United Methodist Church Voice and Data Wiring Logic Diagram-1 and Cedar Park First United Methodist Church Voice and Data Wiring Logic Diagram-2 for more specific location information.
** See the CPFUMC Network Devices List for more details.