FPC - Cybersecurity Policy - May 2026

Ensuring the security of online platforms is crucial for churches. This policy establishes guidelines for password protection, data encryption, safe internet usage, and measures to prevent hacking or unauthorized access.

The purpose of this policy is to establish guidelines and protocols to protect the confidentiality, integrity, and availability of the church's digital assets and information systems. This policy will ensure the secure handling and storage of sensitive data, as well as the prevention, detection, and response to cyber threats and incidents.

This policy applies to all members, employees, volunteers, and third-party vendors, who have access to First Presbyterian of Waco's information systems, networks, or data, including but not limited to administrative staff, IT personnel (Heart of Texas Network Consultants), and volunteers entrusted with managing or using church technology resources. It shall be the responsibility of the Operations Manager, Head of Staff and the Administration Committee to consult with Heart of Texas Network Consultants or the appropriate consultant group to assess Cyber Security best practices for First Presbyterian. See 4 a.

Policy Guidelines

1. Information Security

    a) Ensure the use of strong and unique passwords for all accounts, regularly changing them at least once a year, and avoiding password reuse.
    b) Implement multi factor authentication (MFA) for accessing sensitive systems and data.
    c) Restrict access privileges to authorized personnel by implementing user access management practices.
    d) Regularly update and patch all software, operating systems, and applications to address security vulnerabilities. (HOTNC)
    e) Regularly back up critical data and store backups in secure and separate locations to ensure data recovery in case of a cyber incident or hardware failure.
    f) Securely dispose of sensitive information by utilizing secure deletion methods or physical destruction.

Cybersecurity Policy Template

2. Data Protection and Privacy

    a) Identify and classify sensitive data stored or processed by the church, ensuring appropriate protections, including encryption, for data in transit and at rest.

b) Comply with relevant data protection and privacy laws, regulations, and best practices.
c) Implement procedures for reporting and managing data breaches in accordance with applicable laws and regulations.

3. Network Security

a) Implement firewalls, intrusion detection and prevention systems, and other security measures to safeguard the church's network infrastructure.
b) Regularly monitor network traffic and logs to detect and respond to potential security incidents and/or access of inappropriate sites.
c) Secure wireless networks with encryption, strong authentication, and network segmentation.
d) Regularly update and patch network devices, including routers, switches, and access points.

4. Security Awareness and Training

a) Annual Cybersecurity assessment.
b) Provide regular cybersecurity awareness training to all personnel to educate them on common cyber threats, safe browsing practices, and methods to identify and report potential security incidents.
b) Promote a culture of security awareness and encourage employees and volunteers to report any suspicious activity or potential security breaches.

5. Incident Response

a) Establish an incident response plan that provides clear guidance on responding to cybersecurity incidents, including the roles and responsibilities of key personnel.
b) Ensure appropriate measures are in place to collect and preserve evidence in case of a cyber incident to support legal or criminal investigations.

It is the responsibility of all personnel to comply with this cybersecurity policy, relevant laws, regulations, and industry’s best practices. This cybersecurity policy will be reviewed and updated on an annual basis or as necessary to address emerging cyber threats or changes in the church's technology infrastructure.