DATA SECURITY

7 STEPS TO MINIMIZE EXPOSURE OF YOUR MINISTRY'S SENSITIVE DIGITAL ASSETS

UMC INFORMATION TECHNOLOGY SUPPORT

Fire and natural disaster – two ways a church's data could be compromised. Unfortunately, identity theft, ransomware, and digital breaches are also ways a church's sensitive assets can be stolen or burglarized. However, there are steps a church can take to minimize the occurrence of digital poaching within its IT systems.

1

IDENTIFY SENSITIVE ASSETS

What information does a church collect? Is it identifiable? Would a thief be able to use it to steal from an individual or organization? Would you want others to know this information about you? Who is this information shared with? How is it stored? Where do you keep your servers? Can someone walk in and create a back door to your network with just a USB drive and some code?

Don't collect personal information you don't need. Only ask for information you need to conduct the work of the church. Use other services such as online giving apps to store banking information that you do not need to operate the church but which the app supplier has a long history with and better capacity to secure. You can't lose what you don't have!

2

LIMIT DATA ACCESS

Since you have identified your sensitive assets, keep the number of persons with access to sensitive assets to a minimum. Determining who needs permission to access the church's digital information should be as rigorous a process as deciding who can be held responsible for having a key to the church building.

Not everyone needs to have access to all the information the church has. Set up accounts with different levels of access. Restrict access to sensitive data you may collect. Limit administrative access to the technology structure both in software and hardware. Some of your users should have Administrator access but most only need User level access. Track changes using access accounts and stop computer viruses from invading your entire network through one user's account. Limit access between computers on your network and between your computers and the internet.

3

INTRUSION PREVENTION SYSTEM

Protect your data from any intrusions outside the building. Update and patch third-party software regularly including operating systems and anti-viruses. Make sure your data security policy ensures procedures for future vulnerabilities that may arise. Have a process for receiving and addressing reports about security vulnerabilities.

Are firewalls set up correctly for your needs or can someone enter your network via the internet and infect your server or gain access to sensitive data? Firewalls allow you to suspend or disable user credentials when an automated brute force attack is detected – programs that type endless combinations of characters until a password is stumbled upon.

4

ENDPOINT SECURITY

Protect your data at each endpoint, including desktops, laptops, and phones. Implement procedures for when the endpoint is nonresponsive for a period of time. Restrict the number of unsuccessful logins attempts to your network.

Ensure endpoint security with those who have remote access to your network. Ensure that the transmission of information from these devices is encrypted. Follow the information to make sure it is secure throughout the journey it takes if it is traveling along an unsecured Wi-Fi hotspot. You may need to institute Virtual Private Networks (VPNs)..

5

MULTI-FACTOR AUTHENTICATION

All persons entering the digital realm of a church's property need strong and different passwords. No longer are words and numbers, even when capitalized and accompanying one's first born, enough! Think sentences with signs and values within them.

Establish procedures to store credentials securely. Make sure people are who they say they are by implementing an authentication procedure.

6 REGULAR DATA BACKUP

Systems fail. Computers crash. A secure and ongoing back up is needed by every church to protect its digital assets. With multiple entry points, this can become complicated but is crucial in defending your church's data.

Create offline backups of important files. Don't leave your laptop, phone or other devices unattended in public. Make sure they have backup for the information stored on them.

7 DATA SECURITY POLICY AND PROCEDURES

Every church needs a "Data Security Policy," laying out all the rights and responsibilities of all church staff and volunteers as it pertains to the digital and physical data that the church collects or has access to. You may need to have such a policy to be compliant with federal regulations.

These seven steps work together to provide a protective wall of security that works with your church's IT infrastructure to provide the administrative processes it needs to run smoothly and efficiently to do the ministry that God has called your congregation to participate in. Make sure you have what you need to manage securely the data your church has.

GCFA has an experienced and well-trained, up to date, IT department that offers different levels of services for data security at a competitive price. It also hosts the systems you more than likely access to update your church's data, like EZRA and Great Plains. If you are interested in an IT assessment, call us at 615-369-2395.

FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

Contact us at connectionalrelations@gcfa.org or 615-369-2395 for more information on how GCFA can help your church secure your church's digital environment.