BAPTIST INSURANCE SERVICES

Cyber Insurer Requirements for Churches for 21/22 Renewal

The following are requirements from our Cyber Insurer. Churches need to ensure that all areas below are in are part of your processes to maintain cover.

Implement good password hygiene

Passwords are still a valuable way of securing access to systems and applications, when done right.
Each system and application should be accessed using a unique password only known to the user (and not shared with others across the organisation)
Password Managers, some of which are free, are a good way to organise, keep track and update passwords.

Implement Multi-Factor Authentication

Use a secondary factor (either a pin code sends via SMS, a one-time password) to provide an extra layer of security that makes it harder for malicious actor to circumvent, even if the first factor (typically a password) is compromised through a phishing attack. It should be implemented for all users accessing email services (e.g. Microsoft Office 365), finance and account services, website and hosting services, database records, file storage sites and other repositories that contain personal, sensitive, health or financial information.

Implement a regular backup program

Take regular backups of key data and systems, and ensure they are tested. This is critical to the recovery ability following a security breach, particularly where loss of data is involved. Backups should take place weekly.

Anti-malware Software

Install Anti-malware solutions on the device in use, and make sure they are kept up-to-date. While there is a strong reliance on recovery amongst our constituents this should be balance with preventative security measures. Ensure that all software applications in used are patched/updated regularly.
Out of date and vulnerable applications, operating systems and hardware are an avenue of potential security breaches.

Further recommended actions:
Uninstall software that is not in use
Run a vulnerability scanner regularly to identify any vulnerabilities.

Software updates

Regular updates for providers such as Microsoft should be implemented immediately.

Bank accounts

Re-confirm bank account details with call back protocol to ensure bank details are correct.

Remote Desktop Protocol

Remove desktop access should not be activated on your computer systems.

Develop an incident response plan

A key part of cyber security preparedness is making sure a solid, documented plan is in place to respond to security incidents. Constituents should document and test internal responsibilities for dealing with security incidents and identify external parties that could assist with response actions following an incident.

People

Actively implement and encourage awareness on cyber security by leveraging various online resources.