BAPTIST INSURANCE SERVICES

Narrabeen Baptist Church
Cyber Security Policy

Introduction.

The risk of data theft, scams, and security breaches can have a detrimental impact on our organisation's systems, and reputation. As a result, Narrabeen Baptist Church has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose.

The purpose of this policy is to (a) protect Narrabeen Baptist Church's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope.

This policy applies to all of Narrabeen Baptist Church's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data.

Narrabeen Baptist Church defines "confidential data" as:

- Unreleased and classified financial information.
- Congregation member, visitor, volunteer, customer, supplier, and shareholder information.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

All employees are obliged to protect this data.

Device Security.

Organisational Use.

To ensure the security of all company-issued devices and information, Narrabeen Baptist Church employees/volunteers are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from the Operations Manager before removing devices from company premises.
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Personal Use.

Narrabeen Baptist Church recognizes that employees may be required to use personal devices to access organisation's systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees/volunteers are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

We also advise employees/volunteers to avoid accessing internal systems and accounts from other people's devices or lending their own to others.

When new hires receive company-issued equipment they will receive instructions for:

- Filevault disk encryption setup
- 1Password management tool setup
- Installation of Bitdefender antivirus/anti-malware software

They should follow instructions to protect their devices and refer to the administrative team if they have any questions.

Email Security.

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Narrabeen Baptist Church requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for inconsistencies or give-aways (e.g. any significant grammatical errors, capital letters, excessive number of exclamation marks.)
- Avoid clickbait titles and links (e.g. offering prizes, advice).
- Contact the IT department regarding any suspicious emails.

Manage Passwords properly.

Password leaks are dangerous since they can compromise our entire computer network. Not only should passwords ne secure so they won't be easily hacked, but they should also remain secret.
For this reason, we advise our employees/volunteers to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays)
- Remember passwords, or use the 1Password app instead of writing them down. If employees need to write their password, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in person is not possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- All system-level passwords (e.g. enable, application administration accounts, and so on) must be changed on an annual basis.
- It is recommended all user-level passwords (e.g. email, web, desktop computer, and so on) at to be changed at least every quarter.
- Users must not use the same password for various access needs.

Remembering a large number of passwords can be daunting. We use 1Password, a management tool which generates and store passwords. Employees are obliged to create a secure password for the tool itself, following the above mentioned advise.

Transferring Data.

Narrabeen Baptist Church recognizes the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

- Avoid transferring sensitive data (e.g. customer/ member information, employee/volunteer records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our administrative team for help.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Immediately alert the administrative team of any breaches, malicious software, and/or scams.
- Our administrative team must investigate promptly, resolve the issue and send an alert to all employees if necessary.

Remote Employees.

Remote employees must follow this policy's instructions too. Since they will be accessing our Narrabeen Baptist Church's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Data Backup.

Backups are helpful against phishing, ransomware, and insider threats alike. If something goes wrong, having a backup is essential to restore lost files and emails. To protect Narrabeen Baptist Church from loss of information and damage to your reputation, you will need to:

1. Backup regularly
2. Store the backup offsite and offline.
3. Ensure backup data is encrypted with a password and stored in physical secure location.
4. Test your backup to make sure they work as expected.

"***Hardware failure, theft, or malware infection (such as the cryptolocker ransomware attack) can make recovering data that tis critical to your organisation expensive or impossible. To avoid this, you need to back up your data."***

Backup Methods	***Advantages***
Full Backup	✓ All of the data on your computer is backed up including files, applications and operating systems. ✓ Facilitates a complete restoration of the computer
Partial backup	✓ Enables you to select the files you want to Backup ✓ Requires less storage than a full backup. ✓ The backup process takes less time than a full back
Differential backup	✓ A full is undertaken before the first differential backup ✓ Backs up any files that have changed since the previous full backup ✓ Enables full recovery, using the full backup and one differential backup.
Incremental backup	✓ Similar to the differential backup – a full backup is undertaken before the first incremental backup. ✓ Enables full recovery ✓ Take less time to complete each backup, compare with full, partial or differential backups

Choose your backup storage option(s) There are several ways to store your backups, but essentially, they fall into two main categories:

1. Physical storage devices, such as external hard drives; or
2. Online backups, such as cloud-based data storage solutions. You may decide to use either or both backup storage options.

Disposal.

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives and other storage media may contain sensitive information/data. In order to protect our organisation's data, all storage mediums must be properly erased before being disposed of. However simply deleting or even formatting data is not enough. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

When Technology assets have reached the end of their useful life they should be send out for proper disposal. All data should be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks

Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. Narrabeen Baptist Church's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

Review and Respond

Periodic Cyber Security Assessments

Narrabeen Baptist Church will conduct periodic assessment (at least annually) to detect potential system vulnerabilities and to ensure that cybersecurity procedures and systems are effective in protecting confidential members/customers information.

Response to Cyber Security Incidents

Narrabeen Baptist Church will respond to data breaches depending on the type and severity of the incident. In doing so the organisation will:

- Contain and mitigate the incident/ breach to prevent further damage
- Evaluate incident and understand potential impact
- Implement a disaster recovery plan (if needed)
- Determine if the personal information of members/clients was compromised and notify effected members/clients of the date the organisation becomes aware of this breach.
- Enhance systems and procedures to help prevent the recurrence of a similar breach
- Evaluate response efforts to the update response plan to address any short comings.

Appendix A – Internal Threat Risk Assessment

Internal Threat	Risk Level	Response
Intentional or inadvertent misuse of customers/members information by current employees	Medium	1) Dissemination of, and annual training, on privacy laws and organisations privacy policy. 2) Employment agreements amended to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment. 3) Employees encouraged to report any suspicious or unauthorized use of information. 4) Periodic testing to ensure these safeguards are implemented uniformly
Intentional or inadvertent misuse of customer information by former employees subsequent to their employment	Low	1) Require return of all customer information in the former employee's possession (i.e., policies requiring return of all organisation property, including laptop computers and other devices in which records may be stored, files, records, work papers, etc.) 2) Eliminate access to customer information (i.e., business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords, etc., and maintain a highly secured master list of all lock combinations, passwords, and keys. 3) Change passwords for current employees periodically. 4) Send "pre-emptive" notices to clients when the organisation has reason to believe a departed employee may attempt to wrongfully use customer information, informing them that the employee has left the firm. 5) Encourage employees to report any suspicious or unauthorized use of customer information. 6) Periodic testing to ensure these safeguards are implemented uniformly.
Inadvertent disclosure of customer information to the general public	Low	1) Prohibit employees from keeping open files on their desks when stepping away. 2) Require all files and other records containing customer records to be secured at day's end. 3) Use password screensaver software to lock a computer if it has been inactive for more than a few minutes. 4) Change passwords for current employees periodically. 5) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 6) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 7) Encourage employees to report any suspicious or unauthorized use of customer information. 8) Periodic testing to ensure these safeguards are implemented uniformly.

Appendix B – External Threat Risk Assessment

External Threat	Risk Level	Response
Inappropriate access to, or acquisition of, customer information by third parties	Low	1) Install firewalls for access to organisations internet site. Include privacy policy on the site. 2) Require secure authentication for internet and/or intranet and extranet users. 3) Require encryption and authentication for all wireless links. 4) Train employees to protect and secure laptops, handheld computers, or other devices used outside the office that contain or access customer information. 5) Install virus-checking software on all laptops, desktops and servers, and scan all incoming and outgoing e-mail messages. 6) Establish uniform procedures for installation of updated software. 7) Establish systems and procedures for secure back-up, storage and retrieval of computerized and paper records. 8) Establish procedures to ensure external points of entry to the office are closed, locked and inaccessible to unauthorized persons when the office is closed. 9) Physically lock or otherwise secure, all areas in which paper records are maintained. 10) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 11) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 12) Encourage employees to report any suspicious or unauthorized use of customer information. 13) Periodic testing to ensure these safeguards are implemented uniformly.
Inappropriate use of customer information by third parties	Low	1) Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices. 2) Provide all third-party service providers to whom contractual access to premises or records has been given a copy of the Privacy Policy. 2) Require all such third-parties to adhere to the Privacy Policy, agree to make no use of any information on your customers that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the organisation for any inappropriate use of customer information. 3) Require all such third parties to return all customer information and all other organisations property at the completion or termination, for whatever reason, of the agreement between the organisation and the third-party. 4) Prohibit access to customer information (i.e., disabling remote electronic access; invalidating voicemail, e-mail, internet, passwords, etc., if applicable) to all such third-

		parties upon completion or termination, for whatever reason, of the agreement between the organisation and the third-party. 5) Change passwords for current employees periodically. 6) Send “pre-emptive” notices to clients when the organisation has reason to believe a terminated third-party service provider may attempt to wrongfully use customer information, informing them that the agreement with the organisation is no longer in effect. 7) Encourage employees to report any suspicious or unauthorized use of customer information. 8) Periodic testing to ensure these safeguards are implemented uniformly.

Disclaimer:

This policy template is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local, state or federal laws and is not a legal document. The author does not assume any legal liability that may arise from the use of this policy.