Policy Location:	GSA - 21	Created: 7/23/2024
Title:	Data and Computer Security	Revised: (date)
Policy Owner:	Administration Shared Ministry Team	

Associated Documents: Associated Documents: GSA – 1 Administration Shared Ministry Team Policy
Last Reviewed:

Guidelines

Protected Information

Throughout these guidelines, we refer to Protected Information. Here are the types of information that fall into this category.

1. Personal Information includes social security, credit card, or bank account numbers of individuals, and health data. This is generally protected by law. Think about employees, donors, etc.
2. Confidential information is anything a reasonable person would recognize as sensitive or potentially damaging and should generally be protected.
3. Information about minor children, including routine contact information, pictures, etc. might need to be protected, especially if the information itself implies the person is a minor child.

Data Security

1. If you keep paper or electronic records with Protected Information, guarantee that only trusted and authorized persons have access to that information. Don't retain social security, credit card, or bank account numbers of individuals unless it's absolutely essential to conduct the business of the congregation. Destroy it when it's no longer essential.
2. If Protected Information is on a computer:
    1. Require use of a strong password to use the computer. A strong password is at least 12 characters long and includes upper and lowercase letters and digits. (That's almost a million trillion possible combinations.) It does not include names, dictionary words, birthdays, or obvious sequences of numbers. Recent research shows that the best protection comes from a long password that conforms to the rules above.
    2. Passwords should be changed at least every 6 months.
    3. Always change the password whenever anyone loses their authority to access the computer.
    4. Set the computer to lock automatically if it's not used for 10 minutes.
    5. If possible, encrypt the files or folders that contain Protected Information, or encrypt the entire disk drive. If you use encryption, make sure you have a copy of the password stored safely. **Encrypted data cannot be recovered if you lose the password**.
3. If Protected Information is in paper files, lock the files in a cabinet and strictly control who has the keys.
4. Never include Protected Information in an email or an email attachment. Those can be easily snooped by anyone on the Internet.
5. All valuable data (not just protected Information) stored on your computers should be backed up periodically (e.g. weekly). If Protected Information is included in the backups, the backups should be encrypted and removable media should be stored in a locked location.

Hardware and Software Security

1. Extra laptops should be kept in a locked cabinet or secured with a locking cable.
2. All computers should have virus detection software installed and automatically updated every day the computer is used.
3. All software on your computers should be kept up-to-date, especially security updates. This includes your anti-virus software, and operating systems. Most computers come with an update service included and turned on. Don't disable it and do allow it to run.
4. Every computer that can connect to the Internet should have software called a firewall. A firewall is included and turned on in every new computer. Don't disable it and do allow it to be updated.
5. If you have networking equipment (e.g., cable modems, wireless routers), change both the default administrator and network access passwords on each piece of equipment when it's installed.
6. Passwords to computers, network equipment, software, files, and online accounts should be stored in an encrypted and password-protected database. Don't write passwords on paper or post-its, and don't send them in emails.

A Note About Virus and Malware Protection

After doing all of the above, the first line of defense is…. YOU. Watch out for emails, websites, and popups that try to get you to:

- divulge confidential information.
- download something onto your computer.
- allow a scan of your computer.

Never click on a link or an attachment in an email that you aren't expecting, even if it appears to be from a friend. Your friend's computer may be infected and send a virus your way without their knowledge. If in doubt, contact the sender.