Diocese of Des Moines
Information Systems Security Best Practices
Quick Start – Minimum Requirements

1. Have a data backup program in place and current on all computers.

   Resources:

   - Windows 10 System Image Backup: https://www.windowscentral.com/how-make-full-backup-windows-10
   - *Datto Corporate: https://www.datto.com/file-backup-and-sync
   - Carbonite: https://www.carbonite.com/

2. Utilize a cloud storage service for data.

   Resources:

   - Onedrive: https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage
   - Google Drive: https://www.google.com/drive/

3. Install & activate a firewall on every computer/network.

   Resources:

   - Microsoft Security Essentials: https://support.microsoft.com/en-us/help/14210/security-essentials-download
   - Zone Alarm Firewall: https://www.zonealarm.com/software/firewall/
   - Privatefirewall Firewall: http://www.privacyware.com/
   - *Fortinet Firewall: http://www.fortinet.com/
   - Comodo Firewall: http://personalfirewall.comodo.com/

4. Install, activate, & maintain updates of an anti-virus program on every computer.

   Resources:

   - *Webroot antivirus: https://www.webroot.com/us/en/home/sem/brand
   - AVG antivirus: https://www.avg.com/en-us/
   - Norton Antivirus: http://us.norton.com/
   - McAfee Antivirus: http://www.mcafee.com/us/
   - Kaspersky Antivirus: http://usa.kaspersky.com/
   - AVAST Antivirus: http://www.avast.com/

5. Consider utilizing Endpoint Detection and Response (EDR).

   Resources:

   - CrowdStrike EDR: https://go.crowdstrike.com/
   - *Carbon Black EDR: https://www.vmware.com/products/endpoint-detection-and-response.html

6. Install, activate, & maintain updates of an anti-spyware/anti-malware program on every computer.

Resources:

- Spybot Search & Destroy AntiSpyware: https://www.safer-networking.org/compare-spybot-editions/
- Spyware Doctor Antispyware: https://spyware_doctor.en.downloadastro.com/

7. Utilize a spam filter application to guard against unwanted, harmful emails.

Resources:

- Spam Assassin Email Filter: http://spamassassin.apache.org/
- Appriver Email Filter: http://www.appriver.com/
- Email Filter: www.mailwasher.com

8. Utilize social engineering training for employees.

Resources:

- *Knowbe4: https://www.knowbe4.com/
- Ninjio: https://ninjio.com/lp4c-esecurityplanet/

9. Enact a password requirement policy.

- Enforce password activated screen savers/hibernate
- Enforce password protection (i.e. do not share passwords)
- Enforce password strength requirements (At least 8 characters, combination of Upper and lowercase, numbers and special characters

  Example: 0314gMd1oce$e
- Enforce password refresh timelines (minimum every 90 days)
- Use a password manager program such as “Last Pass”.

10. Enable multi-factor authentication (MFA)

The goal of MFA is to provide a multi-layered defense system. This helps ensure that the users who access your system are who they say they are. Even if one factor is compromised, there are still more barriers to breach. For example, if someone’s computer password is stolen, the thief would still need more than just that information to break into the account.

Examples:

- Google Authenticator (an app on your phone).
- SMS text message with a code.
- Soft token (also called software token).
- Hard token (also called hardware token).
- Security badge.

11. Follow online banking security guidelines.
    - Utilize a stand-alone computer for any online banking transactions with your financial institution
    - Do not access any other internet functions from this computer (including email)
    - Follow Internal Control & Separation of Duties guidelines
    - Limit overdraft protection to maximum of $250.

*Currently in use at diocese.

Use of all products above depends on every computer running a current, fully updated operating system (Windows).