Diocese of Des Moines
Information Systems Security Best Practices

Information System security is not a one-time project or expense. It is an ongoing process. These guidelines are meant to assist your organization in working towards Information Systems security.

Personal Computer (PC) Security

Firewall – Every computer and network must have a firewall installed and activated.

- Firewalls assist to keep hackers from using your computer to send out your personal information without your permission.
- Basically, it acts as a guard watching for outside attempts to access your system and blocking communications from and to sources you don't permit.
- Many operating systems and hardware devices (routers) come with a built-in firewall.
- To ensure your firewall is effective, ensure it is turned on, properly set up and updated regularly.

Antivirus – Every computer must have antivirus software installed and activated.

- Antivirus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses and then deleting them.
- Antivirus software must be updated routinely.
- Most commercial anti-virus software includes a feature to automatically download updates when you are on the internet. When deciding on a brand of software, keep in mind that good antivirus software should recognize current viruses, as well as older ones; effectively reverse the damage; and update automatically. Only one antivirus software program can be installed at one time, multiple software installations will work against each other.

EDR – Endpoint detection and response.

- Endpoint detection and response or a Next-Generation Antivirus (NGAV) software (NGAV) software (Crowdstrike, Cylance, Carbon Black) should be used to secure all system endpoints..

Antispyware – Every computer must have antispyware installed and activated.

- Antispyware software helps protect your computer from malicious spyware that monitors your online activities and collects personal information while you surf the web.

- Since the sophistication of spyware programs is increasing, consider using two different antispyware programs to offer increased protection.
- The low end antivirus only solutions are no longer sufficient to protect your systems. Use an Antivirus in conjunction with antispyware and firewall applications.

AntiMalware – Every computer must have antimalware installed and activated.

- Antimalware software protects your system against trojans, scareware, worms, adware, botnets, rootkits, keyloggers and crimeware. These are programs that can be downloaded to your computer without your knowledge.
- You can install multiple anti-malware software applications on the same computer.

Spam Filters – A spam filter is highly recommended.

- Spam filter software is installed on a mail server that blocks unsolicited emails.
- Users are often able to set varying levels of filtering so wanted emails are not blocked. Some spam blockers will hold emails they detect as unsolicited in a downloadable section until they are passed through a variety of spam filters.
- Anything that has been blocked is often set aside for inspection for a certain number of days. Spam emails are no longer just annoying, they are dangerous.

Screen Saver – Hibernate – Password Protect – Password activated screen savers must be used to lock computers after a period of inactivity.

- Require the combination of key strokes CTRL+ALT+DEL to logon. This provides an additional security layer requiring the user to physically be at the computer to log on.

Passwords: Strength, Length, Security, Sharing, Forced Changes – Protect your passwords by keeping them in a secure place and out of plain view.

- Do not share your passwords.
- Strengthen your password by making it harder for hackers to figure out.
  - Use passwords that have at least eight characters and include numbers and symbols.
  - Never use your personal information or login name as a password.
  - Change your passwords regularly (every 90 days at a minimum).
  - Passwords should not be the same as any of the previous six passwords.
- Use different passwords for each online account you access.
- Use different passwords for different websites and systems.
- Keeping multiple complex passwords means that it might be necessary to consider a password management tool.

Software Application Updates (including Microsoft Windows & Office; Adobe, etc.) – Every organization should have a documented maintenance routine for keeping applications up to date.

- Hackers take advantage of unsecured web browsers and operating system software. Your operating system may offer free software patches that close the holes in the system that hackers could exploit.
- Common operating systems (Windows) can be set to automatically retrieve and install patches for you.
- If not, make regular visits to your system's manufacturer website and update your system with defenses against the latest attacks.
- Or utilize a third party system scanner to scan and notify you of updates available. Without these updates, your system will not be well protected against new cyber threats.

Data Storage –

- Recommend encryption of all sensitive and confidential information stored in your systems and networks.
- If data is not encrypted, servers that store sensitive and confidential information should be segregated from the rest of the network.
- Access to this data should be controlled with role-based assignments.

Backups – Every organization should have a documented and tested "Data Backup and Disaster Recovery Plan in place.

- Highly recommend usage of a reputable cloud storage service for backup of all data.
- No system is completely secure. It is important to copy important files onto a removable disc and store securely in a building other than where your computer is located.
- Always keep your original software start-up disks handy and accessible for use in the event of a system crash.
- Data backups should run on a set schedule, daily or weekly and data should be segregated and/or disconnected from your network in such a way to reduce or eliminate the risk of the backup being compromised in a malware or ransomware attack that spreads throughout your network.

User Access Rights – Local/Power User/Limited – Only an "Administrator" login should be able to modify any system files.

- You can set the limited user access rights in the Control Panel – User Accounts –Properties of the User – Group Membership.
- Local user access rights apply to the computer itself and everything that runs on that computer.
- Disable the local Administrator login OR lower the privileges for that login. Then create a new local account on that device and name it something other than "Administrator". Establish a password for that new local account and use it for any administrator types of processes. This lowers the chance of someone without authority gaining access to the original system administrator login with full access rights.
- Only log into a workstation as an "Administrator" with full access rights when necessary to download software applications.
- Other daily users of the PC should have their own login, with limited access rights.
- Some software applications require Power User level access which still limits the ability to install any type of software to the computer, including viruses.

Application Access Rights (Such as Financial Information) – Application Access Rights apply to the specific software program that you are using.

- Full application access should be granted only to those who need it to perform their duties.
- Be sure to assign an "Administrator" of security for financial software applications in use.
- Monitor the access that each user login has to the private financial or personal data. Do not use one generic login with a well-known password.
- Any individual who will have access to sensitive information should have a background check completed.
- Access to this information should be strictly limited to individuals who have a business reason to see it.

Application .exe files – Only "Administrator" login should be able to run software application .exe (executable) files.

- Attachments to emails often contain an .exe file that triggers a virus to enter your computer.

Employee training on security (conferences, classes, webinars, internal meetings) –Implement a Computer Usage / Security Policy.

- Employees and volunteers must be trained to ensure security, confidentiality, and integrity of sensitive information is maintained.
- All employees, particularly those with financial or accounting responsibilities should complete social engineering training.
- Remind staff on a regular basis of policy to keep information secure and confidential.
- Impose and follow through with strict disciplinary measures for policy violations.
- Ensure your I.T. individuals are up to date on the latest technology.

Signed Employee policy – Enact an Email and Internet / Computer Usage Policy.

- All employees should be given a hard copy to read and required to sign and date that they have read and understand the policy.

Termed Employee Policy – Every organization should have a documented procedure in place which includes that terminated employees or volunteers should have their passwords deactivated immediately.

Destruction of electronic files & emails. Archiving policies –If you collect, store, host, process, control, use or share any private or sensitive information in either paper or electronic form, or biometric information or data such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person, these records must be stored securely if physical documents or secured on restricted storage drives if in digital format. Ensure disposal of sensitive information is done in a secure manner.

- All paper records should be shredded in a manner that they cannot be read or reconstructed.
- Data must be erased when disposing of computers, disks, CD's, hard drives, laptops, cell phones or any other electronic devices containing sensitive information.
- There are software applications that will certify all data has been erased. Or, you can physically destroy the hard drive, memory cards, or disks.
- Archiving policies reflecting USCCB guidelines should be in place for specific categories of data with destruction timelines and confirmation ofdestruction.
    - This can be found in the *Parish and School Resource Manual,* chapter II, page 22

- http://www.dmdiocese.org/resourcemanual.cfm

- Delete everything that you do not need. Email archives are sometimes targeted by data thieves.
- A data management program is key to keeping old data organized and safe.

Third-Party Contracts/Vendor: Maintain a current signed contract for all third party vendors.

- Have the contracts reviewed by legal counsel if necessary.

Hardware: Each organization should maintain a hardware replacement schedule based on general hardware depreciation rules. Older hardware is not as secure and or reliable.

Email Security

Phishing – "Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with on a regular basis (i.e. your financial institution, an Internet Service Provider (ISP), a government agency).

- This is the "phishers" way of tricking you into divulging personal information so they can steal your identity.
  - Never open unsolicited email messages
  - Don't open attachments from people you don't know or don't expect
  - Don't reply to or click on links in email or pop-ups that ask for personal information via email
  - Legitimate companies never ask for this information in this manner. Verify the request by calling the company directly; however, use a contact number on a recent statement instead of one given on the email.
- You can confirm a URL link in an email by hovering your mouse over the link to verify where you will be directed on the internet. Make sure the web address displayed is indeed a site you wish to be directed to.

Attachments – A virus sent over email cannot damage your computer without your help.

- Never open an email attachment unless it is from a known source or you know what it contains.
- When sending emails, help others trust your attachments by including a message in your text explaining what you are attaching.

Encryption – Any sensitive information sent over the internet via email or stored on mobile devices should be encrypted.

- You can encrypt individual email messages by setting that configuration option within your email account. By default, email messages are NOT encrypted.

- In Microsoft Outlook, that setting is located within the Tools – Options – Security –Encrypted Email window. Check the box for "Encrypt contents & attachments for outgoing messages."
- For highly confidential, private messages, consider using an encryption service for individual email messages.

Suspicious Emails: When in doubt, DELETE!

Multi-Factor Authentication:

- Every user of an email account should have MFA set up on the account. This requires a password and some other form of identification.

Mobile Devices

Laptop – Hard Drive encryption/safeguarding appliance – Encrypt the hard drives of all mobile devices.

- Anywhere from 500,000 to over 1,000,000 laptops are lost or stolen in the United States each year. In some cases, the data on the hard drive is often more valuable than the machine itself.
- To determine if disk encryption is something you should be considering, simply ask yourself if your laptop contains anything you would not want posted publically on the internet. If the answer to this is yes, then encryption is worth considering.
- There are many Open Source (free) disk and file encryption software programsavailable as well as licensed products. Many of those programs also encrypt data on external hard drives and USB devices.

Cell Phones/Smart Phones – Implement a mobile device use policy that includes the use of cellphones for business purposes.

- Include in the policy information about personally owned equipment versus organization owned equipment.
- Be clear on what types of organizational information can be accessed via cell phone and how that information is transmitted and/or stored.
- Safeguard personal health information, credit card numbers, bank account numbers, etc.
    - Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password protect your device so that nobody else can use it or view your information.
    - Store your device in a secure location.
    - Frequently delete text messages, especially those from your financial

institution.

- Never disclose via text message any personal information (account numbers, passwords, social security number, date of birth, etc.)
- If you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile at your bank.
- Download mobile applications (apps) from reputable sources only. Download the most recent version of the app.
- Sign off when you finish using a bank app rather than just closing it.
- Bookmark the official mobile banking site and reference it only.
- Telephone or Voice Phishing: This is known as vishing. This tactic is a phishing attempt made through a telephone call, fax or voice message.
    - If you are uncomfortable continuing a phone call that was not initiated by you, ask for a reference number and call the company using legitimate sources of contact information.
- Text message Phishing: A phishing attempt sent via SMS (Short Message Service) or text message to a mobile device is referred to as smishing. The purpose of text message phishing is the same as traditional email phishing: convince recipients to share their sensitive or personal information.
    - Never disclose via text message any personal information, including account numbers, passwords, or any combination of sensitive information that could be used fraudulently.
    - Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a web site.
    - These messages may be part of a phishing scam conducted by fraudsters to capture your confidential account information and commit fraud.

I-Pads – I-Pads and other tablets or Netbooks should be referenced in your organization's mobile device use policy.

USB's/Flash Drives/External Hard Drives – Limit USB ports and serial ports on networked computers. These are the most common entry points for problems.

- Some organizations eliminate the access to USB ports and serial ports due to this risk.
- You can disable the use of USB ports by changing this setting on the PC through the Control Panel options.
- You can establish a domain policy on the network to prevent all access from any USB storage device.

- In Microsoft Windows operating system, this setting is found in the Device Manager area. You can click the device and disable it.
- Any USB device that will be connected to a networked computer must first be scanned by your antivirus program for any virus or spyware, prior to every connection to the networked computer.
- To scan a USB device, you must plug the device into your computer (do NOT open any files). Then open your antivirus program and choose to scan the port where you have plugged in the USB device. Refer to the Help Menu of your antivirus software program for assistance.

Electronic Banking

Utilizing your Bank's Website – Establish a clear procedure for electronic banking that creates dual controls and minimizes risk from online fraud. Do not depend solely on the bank to protect you. Verify that your financial institution has ample security measures in place to protect your data and the access to your account but each parish/school must take responsibility for its own protection and security.

The following is **mandatory** when utilizing online banking:

- A separate stand-alone computer must be used whenever you are logging onto your bank's website. This can be an older computer, that has been cleared off by a professional.
    - No other internet browsing or email should be allowed on this computer
    - Allow no stored or saved passwords
    - Remove all unnecessary user accounts
    - Remove all non-essential programs
    - Turn off Remote Desktop and Remote Assistance
- Transfers between bank accounts should always be approved by two people. This could be the bookkeeper and the Pastor or Finance Council Member. Both people should sign a form illustrating the approval of this transaction. This authorization should occur before the online transfer is initiated. Determine if your bank can create transfer templates, whereby only specified accounts can be transferred to. This will reduce the risk of fraud and theft but also of accidently typing in an incorrect bank account number.
- After the transfer has been processed, print out a confirmation to attach with the dual authorization form.
- Do not have any overdraft protection on any bank account.

The following are **strongly recommended** when utilizing online banking:

- Ask your bank if they offer any additional security measures, such as Positive Pay, IronKey, and Trusteer Rapport software. Another security measure is utilizing a fob (which would be provided by the bank) to log into the bank's website instead of creating a password.
- Have an employee or Finance Council Member who does not have signatory power on any bank account and view only access, sign onto the bank accounts regularly to look for suspicious activity. It is recommended that at least once a week this person view the activity.

If you utilize ACH as a method of payment or for deposits:

- Upload the ACH file to the bank's website utilizing the stand alone computer. Do not email the file to the bank through normal email channels.
- Ask your bank to notify you either by email or phone for all electronic transactions.
- Have dual authorization for all ACH transactions processed. Similar to the process for bank transfers, two people should sign a form authorizing the ACH transaction. This could be the bookkeeper and the Pastor or Finance Council Member.
- Print out a confirmation illustrating the ACH's successful upload and file this, along with the authorization form, with the journal entry recording the transaction in the general ledger.
- Ask your bank to set up templates to be used for disbursements with the receiving bank account information defined. This might be used for employees receiving paychecks and expense reimbursements.

Internet Usage [Including Social Networking Sites]

Computer Usage Policy (including PC, Internet, Email, Social Networking Sites, Instant Messages) – Draft and implement a Computer Usage Policy that includes internet usage.

- Provide a hard copy to all employees and have them sign that they have read and understand the policy.
- Outline the acceptable use of computer equipment.
- Include a statement that indicates that any data created on organization owned systems remains the property of the organization.
- Be sure to outline those items that are considered Unacceptable.

Web Filters – Install filters to prevent users from accessing forbidden sites.

- You can install web filters directly on a router and then apply the settings to all computers connected on a network.

- Web filters can be applied by site category, or by specific URL addresses. Many filter programs offer a setting for "known" bad sites as well. Apply those settings and monitor them.
- Check a website's reputation before navigating to it. You can also confirm a business website by going to the Better Business Bureau website, BBB.org.

URL's vs. Pop-ups (Alt-F4) – Pay close attention to any URL address that you travel to on the internet. Many times you can hover your mouse over a link in an email or on a website to reveal the URL where you will be taken if you click on it.

- Pop-Up Windows are small windows or ads used to obtain personal information.
  - These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software.
  - Avoid downloading programs from unknown sources on the internet.
- If you receive Pop Up messages while on the internet, you can close the window by clicking on Alt-F4 instead of clicking inside of the pop up box, which many times is a URL link.
  - You can also close down a rogue internet browser window by clicking on Ctrl+Alt+Del on your keyboard, choose Task Manager and click on the Applications tab.
  - Close the internet browser window by highlighting it and clicking on End Task.
  - As a last resort, perform a hard shut down by pressing and holding the computer power button until the machine powers off.
  - Leave the machine off for at least 30 seconds before powering back on.
- Disable the remote login option on the computer if it is not necessary for daily job performance. This setting can be found in Control Panel – System – Remote.

Downloading (.exe files) – Any file with an .exe extension is an executable file and will make changes to the hard drive of your computer. Only download and install legitimate software. Applications should only be installed by an "Administrator" login.

Online Forms (online banking, enter account #, password = form) – Do not save the information you enter into online forms for later use (i.e. bank login forms).

- Ensure the website is secure prior to completing any online forms.
  - Examples include a "lock" icon on the browser's status bar or a website URL beginning with "https:".
  - Read and understand the website's privacy policy to understand how the information you enter will be collected, used, and distributed.

Always log off from any website after making a purchase with your credit or debit card.

- If you cannot log off, shut down your browser to prevent unauthorized access to your account information.

Close your browser when you are not using the internet.

Would you like to "Remember"? Don't save information! Don't save user names! – This data is entered and stored in a file that could be later accessed by someone without authority.

Delete Cookies & Temp Internet Files. Delete History – Establish a maintenance routine that includes these actions on your PC.

- In Windows operating system, you can do this via the Control Panel – Internet Options.
- This should be part of your routine monthly maintenance on your workstation that also includes patching any application updates that may be available.

Social Networking Sites – Establish a clear Acceptable Use Policy for the use of Social Networking Sites that are both related to your organization, and those that are personally owned by organization staff.

- Other users may recognize staff as representing the values of the Catholic Church. Establish "Best Practices" for all kinds of Social Networking including Facebook, Twitter, Instagram, etc.

VPN Access – Establish a policy on organization staff working from home.

- The policy needs to address the type of work that can be done from outside of the organization's network. It should also address the need for security.
- The home computer must pass antivirus/antispyware/antimalware standards before it can be allowed to connect to the organization network.
- The home user must monitor the VPN connected computer so that non-authorized users do not gain access to organization information.
- No banking work should be completed from outside of the secured organization network.
- Multi-factor authentication should be used with all VPN connections.

Wireless Network: Confirm you have secured your wireless network using current WPA2 (wireless encryption protocol).

- WEP is no longer an adequate security protocol.

- Utilize current router hardware. Do not allow unauthorized users onto your wireless network. Your unsecured network can be used for illegal purposes and other computers on an unsecured wireless network can be accessed.

Turn your computer off completely when you are finished using it – do not leave it in sleep mode.

PCI Compliance (Including Credit Cards & ACH)

Policy – Adhere to the Payment Card Industry Data Security Standards released by the Security Standards Council. Any staff with access to data that should meet these standardsshould be familiar with the policy.
Adherence – Work to continuously adhere to each of the standards.
Testing/Proving – Work to continuously test the security of the data and document all standards and procedures that are in place to safeguard this data.

Resources:

Antivirus Programs:
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/
McAfeeAntivirus:http://www.mcafee.com/s/
KasperskyAntivirus:http://usa.kaspersky.cm/
AVAST Antivirus: http://www.avast.com/

Endpont Detection and Response (EDR):
CrowdStrike EDR: https://go.crowdstrike.com/
Carbon Black EDR: https://www.vmware.com/products/endpoint-detection-and-response.html

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

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

Data Backup Programs:

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/

Clowd Storage Providers:

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

Google Drive: https://www.google.com/drive/

Password Management Programs:

KeePass Password Safe management tool:http://keepass.info/

LastPass password management tool: https://lastpass.com/

1Password password management tool: https://agilebits.com/products/1password

Common Software Updates & Security Patches:

Microsoft Updates Site: http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us

Adobe Product Updates Site: http://www.adobe.com/downloads/updates/

Secunia Personal Software Inspector: http://secunia.com/

Microsoft Baseline Security Analyzer: http://technet.microsoft.com/en-us/security/cc184923

Encryption Tools and Hard Drive Erasers:

Windows 10 Bitlocker encryption: https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

WipeDrive hard drive eraser: http://www.whitecanyon.com/wipedrive-erase-hard-drive.phpHardDriveEraser: http://www.harddriveeraser.org/

TrueCrypt Encryption: http://www.truecrypt.org/

Email Spam Filtering Services:

Spam Assassin Email Filter: http://spamassassin.apache.org/

Appriver Email Filter: http://www.appriver.com/

Email Filter: www.mailwasher.com

Web Filtering Tools:

Web of Trust is an add-on to your internet browser that will warn you of questionable websites:http://www.mywot.com/

Barracuda Web Filters: https://www.barracuda.com/company/contactK9Web Protection Web Filters: http://www1.k9webprotection.com/ Net Nanny Web Filters: http://www.netnanny.com/

Web Filter: www.opendns.com

Payment Card Industry (PCI) Resources:

PCI Security Standards Council Site:
https://www.pcisecuritystandards.org/security_standards/index.php

Financial Computing Article: www.komando.com

Resources with Sample Policy Documents:

Catholic Mutual Group Site:
http://www.catholicmutual.org/

User Name: 0084des Password: service Diocese of Des Moines Computer Usage Policy:
https://www.dmdiocese.org/filesimages/Technology/Technology%20Dept%20Docs/Computer%20Usage%20Security%20Policy%20Final%2012%204%202013.pdf

Diocese of Des Moines Social Networking Policy:
https://www.dmdiocese.org/filesimages/Technology/Technology%20Dept%20Docs/Computer% 20Usage%20Security%20Policy%20Final%2012%204%202013.pdf

United States Conference of Catholic Bishops: http://www.usccb.org/index.cfm