Archdiocese of Saint Paul and Minneapolis Information Technology Standards for Parishes, Regional Schools, and Archdiocesan Organizations

Date

[Add Logo]

TABLE OF CONTENTS

Page Number

ABOUT THE STANDARDS

PREFACE

Cyber Security is the responsibility of every person using computer networks, systems, and operating computers either virtually or at the Archdiocese Catholic Center, parishes, schools, and any other archdiocesan organization. Failing to adhere to standard security procedures can result in the loss or theft of parishioner, donor, student, or employee confidential information, which could negatively affect the individuals involved, as well as severely jeopardizing the parish, school, or archdiocese. Criminal attacks can lead to severe damages to any IT network.

Many Cyber Security attacks can be prevented with basic security measures. This document describes industry "Best Practices" for ensuring cyber security and stability.

Cyber insurers are requiring all insured entities have and follow Cyber Security Standards with "Best Practices" to obtain or keep coverage. Insurance industry experts are also speculating that cyber coverage may not be available in the future, due to increasing cyber-attacks. Therefore, cyber security standards and best practice procedures are critical to reducing risk to the parish, school and the Archdiocese of Saint Paul and Minneapolis should coverage no longer be available.

Ongoing reviews of these Standards will be completed as necessary by the Archdiocese of Saint Paul and Minneapolis Cyber Security Task Force.

REQUIRED CYBER SECURITY STANDARDS

The standards below are required for all parishes, schools, and other archdiocesan organizations.

TRAINING

Annual, or more frequent, training of staff about the latest security practices, online threats, and office technology operations is necessary for safe computer and information access, whether this is from onsite personnel or outside consulting. Incorporating a cyber security awareness training program for priests, employees, and volunteers who use computers at the location is critical to the security infrastructure. It is the most effective way to combat poor password practices, phishing attempts, and other cyber threats that could put systems, information, users, parishioner, donors, students, or the location at risk.

The Archdiocese of St. Paul & Minneapolis Cyber Security Curriculum provided by Tokio Marine and available on CMGConnect.org is required to be reviewed **annually** by anyone, other than students (see student recommendations below), that uses parish, school or the organization's computers or accesses parish, school, or the organization's systems. Training MUST be completed for all new hires within 30 days from the date of employment. The Tokio Marine curriculum includes Business Email Compromise; Employee Mistakes, Intro to Data Breaches; Phishing; Ransomware; and Wire Fraud.

It is recommended all students using parish, school or the organization's computers, tablets, iPads, or accessing parish, school, or the organization's systems complete annual cyber security training through classroom instruction.

NETWORK/WORKSTATION DEFENSE

Internet-facing firewalls should only have incoming ports open when needed for email and web servers, when these functions are hosted on site. Firewalls are required. In choosing a firewall it is strongly recommended to have a firewall that will add content filtering, gateway anti-virus and anti-malware, intrusion prevention, Geo Filters, and Botnet Filters.

Workstations must have either the operating system firewall, an anti-virus firewall, or both implemented.

Additionally, networks should be armed with intrusion detection systems to detect anomalous network activity, such as ports scans, network sweeps, and data exfiltration.

WI-FI

It is required that there be no open or unsecured networks. There should be at least two SSID's associated, one for public internet access (guest networks) and one for private office access.

Passwords for public networks should be changed every 6 months.

It is recommended that your organization's Wi-Fi be secured using 802.1x authentication protocol in conjunction with Active Directory be used for access to internal wireless networks. With this in place, a network security key or password is not sufficient for access to the network; an authorized user connecting a piece of hardware to a wireless network will also have to authenticate themselves. This will further serve to give the organization a log of devices connected to wireless networks, and the persons connecting those devices.

If your organization cannot secure your network using 802.1x authentication but your Wi-Fi is password protected, the private network password is **never** given out and only the I.T. personnel should know it.

Access to the private network must be ONLY for organization-owned laptops, tablets, and computers that have a business need to access the office network for file and print services.

Guest networks MUST be used for any equipment not owned by the organization. This includes staff personal mobile devices and computers.

MULTIFACTOR AUTHENTICATION

Multi-Factor Authentication (MFA) is achieved when multiple forms of authentication are used to increase the likelihood that the credentials are from the individual to whom they were assigned. This process reduces the risk of impersonation or the use of compromised credentials by an unauthorized individual.

MFA is a security process whereby users must provide at least two different authentication factors to verify their identities and access their accounts. Below are three types of factors used in combination together resulting in multi-factor authentication:

- Something the user knows (username and password)
- Something the user has (an item the user physically carries with them)
- Something the user is (biometrics: fingerprints, face scan, etc.)

The organization shall take the following appropriate measures to prevent unauthorized access to systems (includes elementary, middle and high school students, except as noted):

- Individuals are required to register a second device, with the exception of elementary and middle school students who may not have access to a second device.
- MFA is required for all externally-exposed applications, where supported.
- MFA is required for remote network access.
- MFA is required for all administrative access accounts, where supported, on all assets, whether managed on-site or through a third-party provider.

ANTIVIRUS AND ANTIMALWARE

The organization shall take appropriate measures to protect computers and portable devices against malicious software. Appropriate measures include the following:

- All information systems should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system. Where operationally possible, organizational PCs should be protected by an automated process that maintains the latest versions of approved anti-virus software.
- Organizational PCs should be scanned at least once a week.
- Users should report any suspected infection that has not been cleaned or quarantined to their IT Helpdesk and follow the instructions received.
- Virus scanning software should be set to automatically clean or delete infected files. If the virus scanning program is unable to clean/delete an infected file, the file that is infected should be quarantined for further review by the administrators.
- All incoming and outgoing email and attachments should be scanned for infections prior to being received by the user or being sent from the organization’s system.

- Personal firewalls and anti-spyware should be implemented where network firewalls or an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) are not implemented.
- Servers should be equipped with an IDS or IPS, where possible.
- Mail servers should have either an external or internal anti-virus scanning application that scans all mail going to or coming from the mail server.
- Local anti-virus applications may be disabled during server backups only where an external anti-virus application continues to scan inbound emails and network traffic while the backup is being performed.

Under no circumstances may any user disable anti-virus software or any of its processes without the express authorization of your organization's IT department. IT personnel should supervise any disablement of anti-virus protection and such disablement should be for the shortest time possible to accomplish the needed objective.

UPDATES AND PATCHES

Workstations and servers owned by the organization must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers.

If a device is no longer receiving security updates, it is obsolete and should be replaced or upgraded in place.

❖ Workstations and Endpoints

Desktops and laptops must have automatic updates enabled for operating system patches. Any exception to the policy must be documented and forwarded to the appropriate supervisor for review.

❖ Servers

Servers must comply with the minimum baseline requirements that have been approved by IT. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the organization's asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the appropriate supervisor for review.

ACTIVE DIRECTORY

It is suggested that a server is used for authentication to access file and print services, and for shared authentication on organization owned systems. Using an Active Directory Domain Controller enforces the use of strong passwords and removes the need for peer-to-peer networks. Peer-to-peer networks are discouraged because they lead to sharing of passwords and increase the chance of spreading computer viruses. Centralized authentication also paves the way for the use of 802.1x-based authentication and two-factor authentication (“2FA”) for stronger protection of wireless networks and remote access to systems**.**

PASSWORDS

Traditional password policies requiring mandatory changes every 90-180 days with password complexity (uppercase, lowercase, symbols) are no longer recommended. It is now recommended to use non-expiring passwords without password complexity secured with Multi-factor Authentication.

❖ Understanding password recommendations

Good password practices fall into a few broad categories:

- **Resisting common attacks** This involves the choice of where users enter passwords (known and trusted devices with good malware detection, validated sites), and the choice of what password to choose (length and uniqueness).
- **Containing successful attacks** Containing successful hacker attacks is about limiting exposure to a specific service, or preventing that damage altogether, if a user's password gets stolen. For example, ensuring that a breach of your social networking credentials doesn't make your bank account vulnerable, or not letting a poorly guarded account accept reset links for an important account.
- **Understanding human nature** Many valid password practices fail in the face of natural human behaviors. Understanding human nature is critical because research shows that almost every rule you impose on your users will result in a weakening of password quality. Length requirements, special character requirements, and password change requirements all result in normalization of passwords, which makes it easier for attackers to guess or crack passwords.

PASSWORD REQUIREMENTS AND GUIDELINES

❖ Password requirements and guidelines

The primary goal of a more secure password system is password diversity. You want your password policy to contain lots of different and hard to guess passwords. Here are the requirements and recommendations for keeping parishes, schools and organizations as secure as possible.

- Maintain a 14-character minimum length requirement
- Don't require character composition requirements. For example, *&(^%$
- Don't require mandatory periodic password resets for user accounts

- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users to not reuse their organization passwords for non-work related purposes
- Require and enforce registration for multi-factor authentication
- Enable risk-based multi-factor authentication challenges

❖ **Password guidelines for users**

Make sure to let users know about these recommendations and enforce the recommended password policies at the organizational level.

- Don't use a password that is the same or similar to one you use on any other websites
- Don't use a single word, for example, **password**, or a commonly used phrase like **Iloveyou**
- Make passwords hard to guess, even by those who know a lot about you, do not use the names and birthdays of your friends and family, your favorite bands, and phrases you like to use

❖ **Some common approaches and their negative impacts**

These are some of the most commonly used password management practices, but research warns about their negative impact.

- **Password expiration requirements for users**

  Password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous password. Password expiration requirements offer no containment benefits because cybercriminals almost always use credentials as soon as they compromise them. Because of this it is recommended to set passwords to not expire. There is one exception; passwords for public networks should be changed every 6 months.

- **Minimum password length requirements**

  To encourage users to think about a unique password, keeping a reasonable 14-character minimum length requirement is recommended.

- **Requiring the use of multiple character sets**

Password complexity requirements reduce key space and cause users to act in predictable ways, doing more harm than good. Most systems enforce some level of password complexity requirements. For example, passwords need characters from all three of the following categories:

- uppercase characters
- lowercase characters
- non-alphanumeric characters

Most people use similar patterns, for example, a capital letter in the first position, a symbol in the last, and a number in the last 2. Cybercriminals know this, so they run their dictionary attacks using the most common substitutions, "$" for "s", "@" for "a," "1" for "l". Forcing your users to choose a combination of upper, lower, digits, special characters has a negative effect. Some complexity requirements even prevent users from using secure and memorable passwords and force them into coming up with less secure and less memorable passwords.

❖ **Successful Patterns**

In contrast, here are some recommendations in encouraging password diversity.

- **Ban common passwords**

  The most important password requirement you should put on your users when creating passwords is to ban the use of common passwords to reduce your organization's susceptibility to brute force password attacks. Common user passwords include: **abcdefg**, **password**, **monkey**.

- **Educate users to not reuse organization passwords anywhere else**

  One of the most important messages to get across to users in your organization is to not reuse their organization password anywhere else. The use of organization passwords in external websites greatly increases the likelihood that cybercriminals will compromise these passwords.

- **Enforce Multi-Factor Authentication**

  Make sure your users update contact and security information, like an alternate email address, phone number, or a device registered for push notifications, so they can respond to security challenges and be notified of security events. Updated contact and security information helps users verify their identity if they ever forget their password, or if someone else tries to take over their account. It also provides an out of band notification channel in the case of security events such as login attempts or changed passwords.

❖ Password Security

All users of the parish, school, or organization’s networks and systems must secure their passwords appropriately. At no time should a user write down his or her password in order to remember it. If a user struggles to remember his or her password, he or she may speak to the organization’s IT department for information on approved password management applications that can securely store a user’s passwords.

Teachers or IT staff should be the password administrators for elementary and middle school students in order to reset passwords for students who may not have access to a second form of authentication.

As a final element of password security, if a user’s password is disclosed to any other person who has not received prior authorization from the organization’s IT department for such access, the user must report the unauthorized disclosure to his or her supervisor as soon after discovery of the disclosure as practicable.

Passwords in parish data systems such as PDS or ParishSOFT or on third party software should be different than the password used for internal systems. Users should enroll in Multi-Factor authentication.

Multi-factor authentication **must** be used for remote access to internal networks.

SOCIAL ENGINEERING

Social Engineering means “the psychological manipulation of people into performing actions or divulging confidential information.”

Confidential information will not be shared with unauthorized individuals. Cyber criminals often attempt to trick employees into sharing confidential information. Any request for information using the following techniques should raise a red flag and require the recipient to verify the requestor:

- Referencing an “urgent matter”, a “forgotten password, a “request for employee W-2 forms” or a “computer virus emergency.”
- Using any form of intimidation from “higher level management.”
- “Name dropping” to give the appearance that it is coming from legitimate and authorized personnel.
- Requiring the release of information that will reveal passwords, model, serial number, or brand or quantity of your resources.

- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.
- Using techniques that declare the requestor to be "affiliated" with organization such as a sub-contractor.
- Using techniques that says he/she is a reporter for a well-known press editor or TV or radio company.
- Using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

❖ Phishing Simulation Testing

Organizations must regularly perform phishing simulations to identify employees susceptible to phishing attacks and should serve as a way of training employees to identify and avoid these threats in the future.

Phishing simulations are performed as follows:

- Send simulated phishing emails to your employees to help identify those susceptible to phishing attacks.
- After the simulation ends a list of employees who failed the phishing simulation is provided.
- Assign online training courses to educate the susceptible employees.

Phishing simulations must be performed semi-annually but are recommended to be performed quarterly. Free phishing simulation testing is provided by ePlace Solutions through Tokio Marine. Contact Catholic Mutual Group’s St. Paul service office for instructions or locate directions on CMGConnect.org<Member Specific Resources<Cyber Security Folder.

❖ Social Engineering Reporting Procedure

If one or more circumstances described above is detected then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

If the identity of the requester CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

If the supervisor or manager is not available, that person MUST contact security personnel.

If security personnel are not available, the person MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor as soon as possible.

WIRE-TRANSFER FRAUD

Wire-transfer fraud is when employees are deceived by criminals to wire money to a bank account controlled by the criminals. These standards require that procedures be established for outgoing wire payments to reduce the likelihood that wire transfer fraud is perpetuated.

❖ **Avoidance Procedures**

These procedures must include the following:

- Establish specific wire instructions with any new business partner who may receive wire payments. These instructions must include the contact information of a designated individual or department at the business partner that can be reached to confirm a wire or a wire transfer change request. At the same time, the organization shall provide the business partner with similar contact information.
- Independently verify over the phone all wire transfer requests and changes to wire instructions using a known and trusted phone number — not one from the current wire transfer request. The contact information provided in the request must not be used to verify the request.
- Complete all wire transfers and any new instructions or changes to existing wire instructions with dual control (e.g., two employees).
- Designate employees who are authorized to send wire transfers. All other employees are prohibited from wiring payments.
- Set up wire rules with your financial institution that dictates who may initiate, release, or approve outgoing wires with the bank. There must be at least two people involved in this process and one of them must be an authorized check signer on the account.
- Treat all changes to wire instructions and urgent requests to wire funds with skepticism and presume them fraudulent until verified for authenticity.
- Establish procedures for reporting suspected fraudulent wire transfer requests so that other employees may be alerted to the scam.
- Verify with your organization’s bank to confirm both the account number and the name on the account before sending a wire.
- Establish internal procedures for any internal requests to wire funds or change wire instructions and train employees accordingly.

❖ Reporting Procedures

This policy requires that procedures be established and followed if the organization has been the victim of wire fraud. Reporting procedures can be found on page 19 of this document, on CMGConnect.org in Member Specific Resources and by contacting Catholic Mutual Group’s St. Paul service office.

These procedures include:

- Notify the receiving bank and request that a freeze be placed on any remaining funds.
- Promptly notify the cyber insurance carrier.
- Notify law enforcement after seeking advice of counsel.
- Investigate whether the organization’s email system may have been compromised.
- Ask business partners to investigate whether their email systems may have been compromised.

PROTECT SENSITIVE INFORMATION

All users must comply with the following to protect sensitive information:

- Promptly report the theft, loss, or unauthorized disclosure of proprietary or confidential information.
- Encrypt all information considered sensitive or vulnerable. This includes outgoing emails.
- Ensure mobile and computing devices that connect to the internal network will be limited to the minimum access necessary to conduct business in order to protect sensitive, proprietary, or confidential information from potential compromise.
- Ensure all computing devices are secured with a password-protected screensaver that activates automatically after 15 minutes or less.
- Manually lock the screen or log off when leaving their computing device unattended.
- Use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
- Safeguard all equipment assigned to their exclusive or shared use, and all equipment within their work area.
- When traveling with laptop computers must always carry them in carry-on baggage and not in checked baggage.
- Only access files that are required for the completion of their job duties.
- Follow the retention schedule, when the retention period is over electronic and physical documents must be destroyed.
- Only share data with authorized people and limit file access.

REMOVABLE MEDIA

Removable media has become less preferred due to the associated risks. Instead, information sharing services like OneDrive and Dropbox are preferred because of their built-in security measures. It is recommended that removable media not be used for sharing sensitive information, unless absolutely necessary for your organization. If necessary, the following procedures must be followed.

❖ Handling Removable Media

The following procedures must be followed when handling Removable Media:

- Information classified as "SENSITIVE" that is copied to Removable Media must be encrypted. Sensitive information should be stored on Removable Media only when required in the performance of your assigned duties.
- Removable Media that contain information classified as "SENSITIVE" shall not be removed from the organization premises unless prior authorization or approval is obtained (authorizers to be determined by the organization).
- When directly transferring Mass Removable Media (e.g., Data Center tapes) containing sensitive information to a third-party, the organization shall request the third party to provide a delivery receipt, including the date and time of delivery to the third party and the name of the person receiving the Mass Removable Media. In cases where the Mass Removable Media is being delivered by a delivery service, the organization shall request from the delivery service a delivery receipt that includes the date and time of the delivery to the recipient and the name of the person who received the delivery from the delivery service, and that receipt shall be sufficient. The above receipts (whether from the third party or from the delivery service) shall be kept on file by the organization.

❖ Removable Media Management

The following protective measures must be followed to protect Sensitive Information:

- Label Removable Media with sensitive information, avoiding specific references to type of content.
- Organizations shall manage the type/quantity of Removable Media purchased for employees and track them as assets by numbering or marking each medium.
- Avoid leaving Removable Media unattended on desks or leaving them inserted in organization computers for any time frame longer than necessary to fulfill business requirements.
- Store Removable Media that contain information classified as "SENSITIVE" in a locked office, safe or locked filing cabinet when unattended.
- Staff may only use removable media provided by the organization.

- Staff may only use removable media containing organizational data in work computers.
- When using removeable media such as USB drives and DVDs, it is important to scan these devices for malware before use.
- If an unknown USB device is found, DON'T USE IT AT ALL; this is a common trick to gain access to private networks.

❖ Disposal of Removable Media

The following measures shall be implemented when disposing of Removable Media that contain Sensitive Information:

- When Sensitive Information stored on Removable Media is no longer required, the recorded Sensitive Information must be deleted in such a way that it is unrecoverable.
- Erasing tools used to delete recorded Sensitive Information must be approved by the person in charge of Information Security.
- If Removable Media containing Sensitive Information is managed by a third-party vendor, the Sensitive Information on Removable Media must be erased in such a way that it is unrecoverable and the third-party must attest to the state of the Removable Media through a signed receipt. Methods used by third-party to erase Sensitive Information on Removable Media should be reviewed by the person in charge of Information Security.

REMOTE ACCESS

It is the responsibility of the organization's employees, contractors, vendors, and agents with remote access privileges to its corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.

General access to the Internet for recreational use through the network is strictly limited to employees, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing the organization's network from a personal computer, Authorized Users are responsible for preventing access to any computer resources or data by non-Authorized Users. Performance of illegal activities through the organization's network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.

Authorized Users will not use the organization's networks to access the Internet for outside business interests.

❖ **Requirements**

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong passwords. All remote access shall be protected by multi-factor authentication.
- Authorized Users shall protect their login and password, even from family members.
- While using an organization-owned computer to remotely connect to the corporate network, it is recommended Authorized Users ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Time-outs on inactive portals or VPN sessions.
- All hosts that are connected to internal networks via remote access technologies must use the most up-to-date antivirus software, including personal computers.
- Authorized users who wish to implement non-standard remote access solutions to the organization's network must obtain written prior approval.

REPORT LOST OR STOLEN DEVICES

Organizations should maintain a full accounting (make, model, serial number, etc.) of technology assets. This includes computers, laptops, hard drives, mobile devices.

It is important to report a lost or stolen device to the person maintaining the location's I.T. who will determine if a remote wipe is possible. Catholic Mutual should also be contacted if the device in question contains confidential information such as donor addresses, phone numbers, donation amounts, student information, password, credit cards, social security numbers, etc.

BACKUP

An effective backup strategy must consider the importance and time-sensitivity of the data. Organizations will follow the industry best practice 3-2-1 backup rule: 3 copies of data on 2 different media with 1 copy being off-site.

❖ **Devices**

Data backups will be made of all devices that contain or collect data, to include at a minimum:

- Servers and their internal disks
- Storage Area Networks
- Desktop PCs
- Notebook PCs

- Devices containing organization’s data

❖ Data Backup Frequency

The frequency of data backups is determined by how frequently and how much a data storage element changes:

- Full backups weekly—all data is backed up weekly and retained for a period specified by the organization.
- Incremental backups daily for changing data. These are retained for a period specified by the organization.
- Off-site journaling is used for immediate backup of critical data that cannot be reconstructed from daily backups.

❖ Data Retention

The organization determines data retention. The retention period is determined by the data element with the longest required retention period on that backup media. If the contents of the media are not known, then the media must be retained for a minimum of 7 years.

❖ Restoring from Backup

The organization should periodically practice restoring from backup. Practice restoring from backup in a test environment will ensure that the organization can restore backups to the production environment if a failure occurs.

❖ Off-site Storage

Data backups will be periodically transported off-site after the backups are created. The off-site facility must meet the following criteria:

- The storage facility is secure.
- The storage facility is climate controlled.
- The data center security is appropriate for media going out and media coming into the system.
- There is a documented chain of custody for backup media from the point it leaves the data center until it is returned.

❖ Data Destruction

Data that has outlived its usefulness to the business or which has been retained for a period that exceeds the legal limits, must be properly destroyed. The following protocols must be followed for all data destruction:

- The media must be rendered permanently unreadable. This is primarily accomplished through physical destruction. Paper documents are shredded, burned, and the ashes pulped. CDs and magnetic media are shredded.
- Documentation must be made as to whom, by what means, when, and what data was destroyed.

❖ **Cloud Services Backup**

Data stored in cloud services like OneDrive and SharePoint has built in data retention, however cloud vendors do not guarantee availability of these backups. Here is the applicable excerpt from the Microsoft Service Agreement:

> *We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored.* ***We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.***

Therefore, it is recommended organizations use third party applications to back up your critical cloud data outside of the cloud service infrastructure.

SUPPORT

Often overlooked, support may be the most critical consideration regarding the location network of any size. Always consider who will implement and review policies, train employees, support the computers or network and how. Ensure that there is a specific agreement with support vendor(s) defining a Support Level Agreement (SLA) that meets the business need. If utilizing the services of an employee in the organization or a parishioner, ensure that the knowledge he or she possesses about the network is well-documented to ensure a smooth transition as needed.

DESKTOP SOFTWARE POLICY

The organization should have clear rules for what employees can install and keep on their work computers. Make sure they understand and abide by these rules by **limiting administrative rights on the location machines**. Unknown outside programs can open security vulnerabilities in your network. Only programs evaluated and approved by the organization should be installed on location devices.

THIRD-PARTY SECURITY TESTING

It has long been an accepted best practice to conduct regular third-party reviews or audits of security posture, with a different set of eyes each time. This ensures that unbiased third parties bring in new areas of expertise each time and provide a snapshot of the risk posture of the organization, and a list of things to consider fixing. Therefore, the organization should conduct regular third-party reviews or audits of security posture.

VULNERABILITY MANAGEMENT PROGRAMS

Vulnerability management programs identify and remediate the security weaknesses created by software vulnerabilities. Vulnerability assessments should be performed annually.

A vulnerability management process consists of five phases:

- Preparation – including determining scope of assets and tools
- Vulnerability scan
- Define remediating actions – determine risks and patching
- Implement remediating actions
- Rescan

Any approved scanning tool must be capable of scanning information systems from a central location and be able to provide remediation suggestions. The tool must also associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the affected scanned system.

WHAT TO DO IF A CYBER INCIDENT IS SUSPECTED

The first few minutes and hours after learning of a cyber incident are critical to a successful recovery. In the event of a suspected cyber-attack or actual cyber security breach:

- Immediately notify your IT Resource Personnel
- Notify the Catholic Mutual St. Paul Service Office 651-290-1605
- During business hours, contact Collin Liston, Associate Claims Counsel for Catholic Mutual Group: 402-514-2405 (Office)/612-636-8655 (Cell)
  OR,
  After hours contact the cyber insurance experts at Tokio Marine HCC:
  1-888-627-8995 or cpl.claims@tmhcc.com – Identify yourself as a Catholic Mutual Member and a participating parish in the Archdiocese of Saint Paul and Minneapolis insurance program

Additionally, the following steps can help to mitigate possible issues:

Cyber Event	Immediate Mitigation Steps
Ransomware infection	• Isolate infected computer from all networks (by unplugging network cable and/or turning off Wi-Fi) • Take picture of the ransomware message on screen (if possible) • Contact your IT department

	• Do not immediately rebuild your system (you might destroy important forensic evidence) • Contact CMG St. Paul Service Office & Claims Counsel
Phishing email attack	• Do not click on link or open any attachment from suspicious email • Call IT representative and forward email to IT for evaluation • Take picture/screen shot of email request/solicitation • Change your email password (strong and unique passphrase) • Contact CMG St. Paul Service Office & Claims Counsel
Malware infection	• Notify IT to have them evaluate and remove malware • Scan network for any other unauthorized files and user accounts • Install anti-virus software and keep updated • Contact CMG St. Paul Service Office
Discovery of unauthorized files or user accounts on server of client	• Close Remote Desktop Protocol (RDP) ports • Change passwords (strong and unique passphrase) • Contact CMG St. Paul Service Office
Lost or stolen device	• Report lost/stolen device to IT immediately • Secure all devices and removable media (passwords and encryption)
Mistaken wire transfer	• Call bank and report details • Attempt to halt transfer • Take picture/screen shot of email request of fund transfer • Contact CMG St. Paul Service Office