

Catholic Mutual...CARES

CYBER SECURITY BEST PRACTICES AND GUIDELINES

Cyber Security is the responsibility of every person using or operating computers at the Pastoral Center, parishes, schools, and any other diocesan facility. Failing to adhere to standard security procedures can result in the loss or theft of parishioner, donor, or employee confidential information, which could negatively affect the individuals involved, as well as severely jeopardizing the parish or diocese. 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 security and stability of office computer networks and is intended to provide the framework for you to create a Cyber Security Policy for your Arch/Diocese. It is recommended that you conduct a regular review of your Cyber Security Policy as technology changes continuously and requires constant review.

The information below will assist you in answering the following assessment and health check questions when it comes to cyber security.

Cyber Security Policies and Procedures:

1. Do you have a documented Cyber Security Policy?
2. Does the policy address items such as two-factor authentication, portable media, mobile devices and wireless access?
3. Are employees aware of, understand and trained to follow the policy?
4. Are the policies and procedures reviewed regularly and kept up to date?

Network and Asset Protection:

1. Do you have adequate firewalls?
2. Are applications regularly patched for updates?
3. Has your asset inventory been documented to include the equipment and who possesses the equipment?
4. Are user accounts controlled, monitored, and protected against unauthorized physical access?

Data Protection and Recovery:

1. Have you defined what types of data need to be protected and at what level?
2. Are appropriate protection and encryption technologies in place?
3. Is data regularly backed up and protected?

Anti-Malware Measures:

1. Do you have adequate anti-malware software installed on equipment?
2. Does the anti-malware software regularly scan to detect malicious files from e-mail, compromised websites and other sources?
3. Are applications regularly patched for updates?

Contingency Planning and Incident Response/Recovery:

1. Can you identify a cyber-security incident when it happens?
2. Do you have a response plan in place?
3. Have you tested recovery processes such as the restore-from-backup scenario for success?
4. Does your plan include a plan for core business activities should a major system failure occur?

TRAINING:

Annual, or more frequent, training of staff about the latest security practices, online threats, and office technology operations are necessary for safe computer and information access. This training can be conducted by onsite personnel or outside consultants. Incorporating a cyber security awareness training program for priests, employees, and volunteers who use computers at their location is critical to the security infrastructure. This is an effective way to combat poor password practices, phishing attempts, and other cyber threats that could put systems, digital information, users, parishioners, donors, students, or the location at risk.

Please see **Appendix A** for a list of suggested on-line trainings and resources.

NETWORK/WORKSTATION DEFENSE:

A firewall is a security device that is used to defend your network against emerging threats by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

Internet-facing firewalls should only have incoming ports open when needed for email and/or web servers, and only when these functions are hosted on site. It is a good idea to have a firewall that will add content filtering, gateway anti-virus and anti-malware, intrusion prevention, Geo Filter and Botnet Filters. These features are often found in lower-end firewall manufacturers. These devices have about a 3-to-5-year life span.

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 port scans, network sweeps, and data exfiltration.

Please see **Appendix B** *Network Security Policy and Usage* for assistance in creating your policy.

WI-FI:

Wireless networks must be password-protected. There should be at least two SSID's (Service Set Identifiers or Network IDs) associated, one for public internet access (guest networks) and one for private office access.

Access to the private network must be **ONLY** for parish-owned laptops, tablets and computers that have a business need to access the office network for file and print services. The private network password is **NEVER** given out and only the IT personnel should know it. Guest networks **MUST** be used for personally owned equipment, including all mobile devices and should be completely segregated from your business network.

It is recommended that 802.1x / two-factor authentication in conjunction with Active Directory (see below) is to 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 parish a log of devices connected to wireless networks, and the persons connecting those devices.

THE “KRACK” VULNERABILITY OF 2017 AND WIRELESS NETWORKS:

Inventory and check ALL wireless-using devices, including mobile devices, and install patches as soon as available. Be prepared to replace devices that do not receive vendor software fixes. Use AES-CCMP for encryption key rotating, not TKIP (Temporal Key Integrity Protocol). TKIP, in conjunction with this vulnerability, allow for additional packet decryption capabilities, and the ability to inject arbitrary traffic into compromised networks.

ANTIVIRUS AND ANTIMALWARE, UPDATES AND PATCHES:

An antivirus software must be installed on every system. It is very important to update operating systems, anti-virus software, anti-virus software signatures, anti-malware software, and browsers regularly. Full malware scans should be done at least once per week.

ACTIVE DIRECTORY:

It is suggested that a server is used for authentication to access file and print services, and for shared authentication on parish-owned systems. Using an authentication server enforces the use of strong passwords and removes the need for peer-to-peer networks, which are discouraged because they lead to sharing of passwords and also 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.

COMPUTER OPERATING SYSTEMS:

Update Windows, Mac, iOS, Android, and Linux system software as soon as patches and/or updates are made available. Linux server systems should be configured to email out patch reports where consoles are not regularly accessed.

Make sure that the software is still supported by the vendor for updates and security patches. Anything earlier than Windows 7 is no longer supported, and Windows 10 versions prior to 1607 are no longer receiving security patches or updates. Mac or iOS software should be kept up-to-date. If a device is no longer receiving update messages, then it's probably obsolete and should be replaced or upgraded.

PASSWORDS:

Passwords can make or break the security of a system. The standard password should include a combination of upper and lower case characters, numbers and special characters such as (!@#\$%) and should be at least 8 characters long. Do not store passwords on paper and stick them to the monitor or under the keyboard. Written password storage, if required, should be protected by lock and key. If you must share a password, then do it in person or over the phone. Never send a password through email. Aim to change a password every 3-6 months. Avoid using the same password on different systems and **DO NOT** use the same password for both email and banking.

Passwords in parish data systems such as PDS or ParishSOFT or on third-party software should also be changed every 90 days. Any time a service like PDS Church Office, Facebook, or Gmail offers a "two-step verification" or "two-factor authentication," use it. When enabled, signing in will require you to also enter in a code that's sent as a text message to your phone or a separate device. This means that a hacker who isn't in possession of your phone won't be able to sign in, even if they know your password. Two-factor authentication should be used for remote access to internal arch/diocese networks, and for wireless access to internal networks. (802.1x)

PHISHING AND OTHER SCAMS:

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

There are many email scams that happen on a daily basis. An email that begins with “Dear Customer” or “Dear youremail@gmail.com” has a high likelihood of being a phishing scheme. Most legitimate emails from coworkers, friends or companies will state a name as a greeting like “Hi John” or “Dear Mr. Doe”. Care must be taken with messages that state that a shipment of something is in progress and “click here” to view the latest progress of the shipment. Don’t click on a link or open an attached file if you are not absolutely confident that it came from a trusted source.

A good practice for email communication is to check the “to” and “from” lines in the email. Make sure that the email is actually from who is noted. If there is any question, then contact the sender via phone or email.

Also, educate users to hover over links before clicking them to make sure that they are actually links to the places on the internet they claim to be.

Please see **Appendix C** *Protecting your Network from Internet/Email Risks* for additional information.

PROTECT SENSITIVE INFORMATION:

Attackers are after personal, confidential information, or personally identifiable information (“PII”), such as: credit cards, social security numbers, donor or student names, email addresses, birth dates, etc. This information must not be sent through regular email. It must be sent through a secure file transfer system or over the phone. This information in physical form, if needed, must be secured in a locked cabinet or safe when not in use. When resting in stasis (storage) on computer systems, all such PII should be encrypted.

Please see **Appendix D** *Data Protection Policy* for additional guidance.

LOCKED COMPUTERS AND DEVICES:

Physical access to equipment such as a server should be limited, kept locked and secured with a key that doesn’t open any other door. For desktops, have a short computer lockout policy, (5-15 minutes), so if a user steps away from their workstation, the PC will auto-lock quickly and request a password. Laptops must also be physically locked up when not in use. Laptops with sensitive information should not be used outside of the workplace unless authorized by management and should make use of whole-disk encryption to protect sensitive data on the move.

SECURE PORTABLE MEDIA:

Portable devices such as mobile phones and laptops should have password access to the network. When using portable media such as USB drives and DVDs, it is important to scan these devices for malware before use. If you find a USB device, **DON'T USE IT AT ALL!** This is a common trick to gain access to private networks. These devices should not be bootable or allowed to directly run install software.

REPORT LOST OR STOLEN DEVICES:

It is important to report a lost or stolen device to the person maintaining the location's IT who can 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:

Regular backup of critical data is mandatory for business continuity. Using an external drive for backup is acceptable as long as the device is removed after the backup process is complete and the device is encrypted. At least two external devices should be used and rotated at least weekly. The rotated device must be kept in the office safe or kept offsite (ideally in a data storage facility).

Backup services to vendors in the Cloud are an acceptable way to keep your data safe, as long as they can restore to a point in time from multiple backups and they utilize encryption.

Test that data can be recovered from the backups at semi-regular intervals. Quarterly is recommended.

DROPBOX, iCloud, ONEDRIVE APPLICATIONS VS. WEB ACCESS:

Dropbox, iCloud, OneDrive and other file sharing applications leave a potential hole in the defense of your computer. A file placed by someone outside your network into a Dropbox share can slide through to the Dropbox storage areas on all shared computers and potentially will not be scanned by the antivirus program. It is recommended to use the web interface for these applications if you allow others to modify data on the drive. Downloading from the web interface will force anti-virus software to evaluate the file and give you better protection. For all file sharing web applications, it is recommended that you set an expiration time for all users. The recommendation would be for 30 days set as a default for all applications unless longer access time is needed for specific projects.

SUPPORT:

Often overlooked, support may be the most critical consideration with regard to 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 location should have clear rules for what employees and volunteers 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 location Business Manager, Pastor, Principal or IT Director should be installed on location devices.

REMOTE DESKTOP PROTOCOL:

In the wake of the COVID-19 pandemic, remote work options are becoming more popular. The security risks, however, are significantly higher. Ensure there is a specific remote work policy that establishes clear rules as well as penalties for noncompliance. Make sure all employee equipment (both personal and company issued) are updated with the latest software version. Strongly consider the use of a VPN when accessing the organizations resources as it will encrypt communications between the remote worker and the organization's environment. Always use a strong password and allow multi-factor authentication (MFA) as an additional layer of protection. Also, ensure that proper safeguards are in place when using video conferencing apps like Zoom.

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 politically unmotivated 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.

WHAT TO DO IF A CYBER INCIDENT TAKES PLACE:

In the event of a suspected cyber-attack, the following steps should be followed in the case of an actual or potential information security breach, including: (a) all losses or disclosures of confidential or sensitive information, (b) all information security violation and problems, (c) all suspected information security problems, vulnerabilities, and incidents, (d) any damage to or loss of location computer hardware, software, or information that has been entrusted to their care.

It is imperative to create a documented containment and response plan. The following steps should be incorporated to your plan.

Step #1: Do not turn off or reboot any systems, but unplug network cables IMMEDIATELY, and/or disconnect the system(s) from the wireless network. Take notes (date; time; who discovered; what tripped the alarm).

Step #2: Report the incident to: (A) designated person per location policy as well as Catholic Mutual Group and Tokio Marine.

**** Please see Appendix E *Cyber Incident Reporting* for additional information on how to notify the proper resources when there is a potential incident.**

Step #3: Instruct reporting personnel not to do anything until an appropriate representative is obtained (specifically the Tokyo Marine insurance claims personnel).

Step #4: After confirmation, secure the scene. Do not allow anyone to take any action on affected systems.

Step #5: Determine if security of sensitive data was breached and, if so, what data elements are included (e.g., name, age, DOB, SNN, medical information).

Step #6: Preserve and protect the evidence.

QUESTIONS:

If you are looking for additional information or have more questions regarding managing cyber risks, please contact your Risk Management Representative at Catholic Mutual.

ADDITIONAL RESOURCES:

- Appendix F – Recommended 3rd Party Vendors
- Appendix G – Operating Systems End of Life
- Appendix H – Cyber Security Tips
- Appendix I – Cyber Security Best Practices for Working Remotely
- Appendix J – Electronic Signatures (e-signatures)
- Appendix K – Using Video Conferencing Services Safely
- Appendix L – Electronic Fiduciary Transaction Requests
- Appendix M – Simple Technology Assessment and Health Check

APPENDIX



Presents our newest addition to the Risk Management video resource library




What's Included?

Catholic Mutual Group is excited to offer this new training series from Tokio Marine, conveniently hosted on our CMG Connect platform. Videos include:

- Phishing
- Ransomware
- Business Email Compromise
- Employee Mistakes
- Intro to Data Breaches
- Wire Transfer Fraud

These six trainings can be combined in a single curriculum or offered as independent titles for individuals in your Arch/Diocese to access.

To have these trainings added to your customized platform, please contact CMG Connect Support at <https://CMGconnect.org/> via the  button located in the bottom right corner of the page.

For more information, please contact your Risk Management Representative

CMGConnect

Go to <https://CMGconnect.org> to select your diocese then click "Go to Diocese".

Previously had an account? If you have done training in the past and have an account, you can use that same username and password to Sign In at the top right of the page.

Sign In

****Please do not fill in the account creation boxes if you have an existing profile.**

New to training? Create a new account by completing all the boxes. This includes address, primary location (site), and how you participate at your location. If you have questions, please contact your parish/school coordinator.

Register for a New Account

Account Personal Affiliation

Enter your first, middle, and last name as they appear on your driver's license or official ID. Do not use prefixes, i.e., Rev., Fr., Sr., Jr., Dom.

First Name * Middle Name Last Name

Username * Password * Password Confirmation *

Next Step

Account Personal Affiliation

Address 1 * Address 2

City * State * Zipcode *

Phone * Email

Date of Birth *

Previous Next Step

Account Personal Affiliation

*Select the Primary Parish/School at which you Volunteer or Work. (Search or scroll down to find your parish.)

Please select

Please Select a Role *

Choose a Role

I participate as a/an: *

Clergy/Religious
 Driver
 Employee
 Volunteer

Previous Register

1. Your main learning dashboard will show you all of the requirements and optional training curriculums that have been customized for your role.
2. Scroll down under Optional Training Curriculums, to locate the *Tokio Marine Cyber Security Series* module.
3. Click **Start** to watch the videos.
4. (Optional) Print a certificate of completion when finished by returning to the dashboard tab and clicking the gray **Print Certificate** button under the finished curriculum.

CYBER SECURITY SERIES

Brought to you by Tokio Marine

Expires Every 1 Years

Tokio Marine Cyber Security Series

Tokio Marine Cyber Security Series

Start

<https://CMGconnect.org/>



CYBER RESOURCES

Welcome to TMHCC cyberNET and Catholic Mutual Group

Catholic Mutual has collaborated with Tokio Marine HCC to bring you valuable cyber resources. This site can help prevent or mitigate the damages from a data breach by providing:

- Tools
- Training
- Best Practices
- Preparing an Incident Response Plan

All of these resources are available at no cost.



CYBER
TRAINING



SAMPLE
POLICIES



INCIDENT
RESPONSE PLANS



BEST
PRACTICES



Stay Current



Assess Your Cyber Resiliency



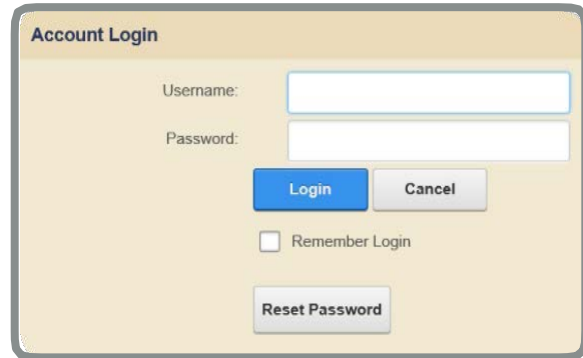
Manage Vendor Risks

Step 1: Accessing Tokio Marine HCC website

Go to www.catholicmutual.org and click on 'Member Login'



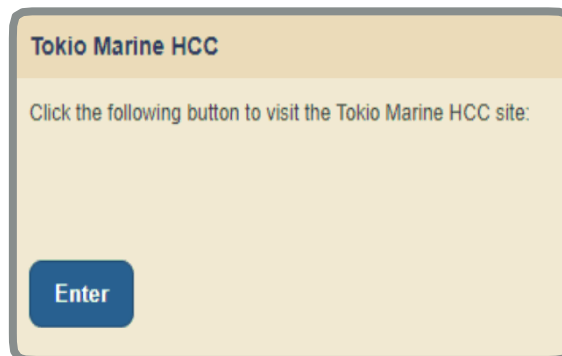
Step 2: Enter Username: _____
Password: _____



Step 3: Click 'Cyber Risk Management' to access Tokio Marine HCC website



Step 4: Enter the Tokio Marine HCC portal



www.catholicmutual.org

Security Awareness Training and Simulated Phishing Platform

Helps you manage the ongoing problem of **social engineering**

KnowBe4 Security Awareness Training

Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.



Baseline Testing

We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.



Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



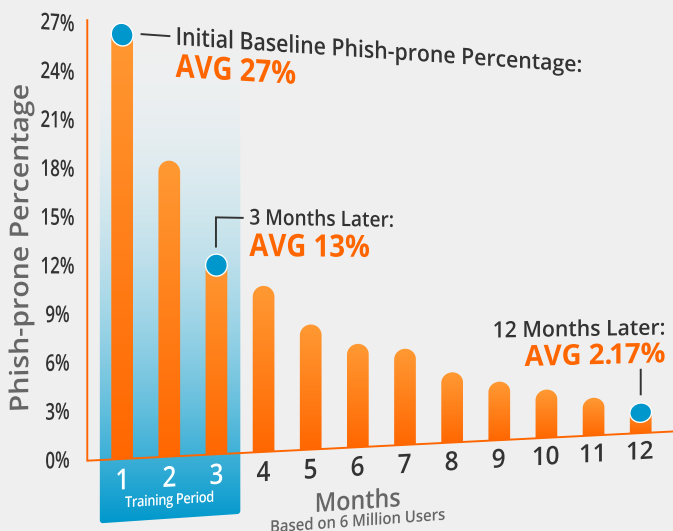
Phish Your Users

Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.



See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



The System Really Works

With KnowBe4's massive database, we analyzed 6 million users over the course of 12 months, and our 2018 research uncovered some surprising results. The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 27%.

Fortunately, the data showed that this 27% can be brought down more than half to just 13% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2.17% on average.

See how your company's phish-prone percentage compares to your peers! **Industry Benchmarking** feature included with your subscription.

Find out How **Effective** Our Security Awareness Training Is

KnowBe4 is the world's largest integrated platform for awareness training combined with simulated phishing attacks. Join our tens of thousands of customers who have mobilized their end users as a last line of defense.

KnowBe4 Security Awareness Training Features



Unlimited Use

We offer three Training Access Levels, giving you access to our content library of 500+ items based on your subscription level. Unlimited access to all phishing features with flexible licensing. No artificial license ceilings and 10% overage allowance. Powerful new features added regularly.



Custom Phishing Templates

Apart from the thousands of easy-to-use existing templates, you can customize scenarios based on personal information, creating targeted spear phishing campaigns, which replace fields with personalized data. **Phishing Reply Tracking** allows you to track if a user replies to a simulated phishing email and can capture the information sent in the reply.



Simulated Attachments

Your customized Phishing Templates can also include simulated attachments in the following formats: Word, Excel, PowerPoint and PDF, (also zipped versions of these files).



Custom Landing Pages

Each Phishing Email Template can also have its own Custom Landing Page, which allows for point-of-failure education and landing pages that specifically phish for sensitive information.



User Management

KnowBe4's **Active Directory Integration** allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes. You can also leverage the **Smart Groups** feature to tailor and automate your phishing campaigns, training assignments and remedial learning based on your employees' behavior and user attributes.



Automated Security Awareness Program (ASAP)

ASAP is a revolutionary new tool for IT professionals, which allows you to create a customized Security Awareness Program for your organization that will help you to implement all the steps needed to create a fully mature training program in just a few minutes!



Social Engineering Indicators

Patented technology turns every simulated phishing email into a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email.



Phish Alert Button

KnowBe4's Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis, and deletes the email from the user's inbox to prevent future exposure. All with just one click!



Security Roles

Allows you to define unlimited combinations of level access and administrative ability that you'd like specific user groups to have. With **delegated permissions** you have the ability to limit roles to only display specific data or allow for the phishing, training, and user management of specific groups.



New! Advanced Reporting Feature

Gives you a collection of 60+ built-in reports with insights that provide a holistic view of your entire organization over time, and dramatically expands instant detailed reporting on a host of key awareness training indicators. Additionally, you can leverage Reporting APIs to obtain data from your KnowBe4 console to create your own customized reports to integrate with other BI systems.



New! Virtual Risk Officer™

The new innovative Virtual Risk Officer (VRO) functionality helps you identify risk at the user, group and organizational level and enables you to make data-driven decisions when it comes to your security awareness plan.



Did you know that **91% of successful data breaches started with a spear phishing attack?**

Get your free phishing security test and find out what percentage of your employees are Phish-prone

www.KnowBe4.com/PST

Catholic Mutual...CARES

Network Security Policy and Usage

OVERVIEW

Internet access to global electronic information resources on the World Wide Web is provided to clergy, religious, employees, volunteers and students to provide ease in obtaining data and technology to assist in their respective ministries, duties or studies.

Our technology systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP), are the property of the diocese/parish/school, and are to be used in support of the mission of the Catholic Church. Maintaining a safe, reliable, and secure system is a collaborative effort involving the participation and support of every individual who uses our information systems. It is the responsibility of every computer user to know and conform to these guidelines.

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment. These rules are in place to protect both the members of our community and the diocese/parish/school. Inappropriate use exposes the diocese/parish/school to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to anyone using the diocese/parish/school technology system, including parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other workers, as well as all personnel affiliated with third parties. This policy has specific provisions for students. The provisions which apply to students, likewise apply to minors who take part in ministries for children and young adults. For clarifications on how this policy applies to minors, the school principal, pastor, or the religious education director is the primary point of contact.

GENERAL USE AND OWNERSHIP

While the network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on parish systems remains the property of the diocese/parish/school. Because of the need to protect our network, management cannot guarantee the confidentiality of information stored on any network device and no rights of privacy exist.

Appendix B – Network Security Policy and Usage

All users are responsible for exercising good judgment regarding the reasonableness of personal use. Commercial use is prohibited. If there is any uncertainty, users should consult the administrator responsible for technology management, the School Principal, or the Pastor.

The equipment, services and technology provided to access the web are the property of the diocese/parish/school. For security and network maintenance purposes, administrators may monitor equipment, systems and network traffic at any time. We reserve the right to audit networks and systems, monitor internet traffic, retrieve and read any data composed, sent, or received on a periodic basis to ensure compliance with this policy.

We rely upon the active cooperation of parents and the responsibility and integrity of students to maintain safe and secure facilities for approved uses of our technology in our school. All users of our computer facilities are asked to live up to that same standard.

UNACCEPTABLE USE

The Diocese/Parish has taken the necessary actions to assure the safety and security of our network. Any individual who attempts to disable, defeat or circumvent security measures is subject to disciplinary action up to and including dismissal. The following are examples of actions and activities that are prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the diocese/parish/school, or use of classified government information.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted video, and the installation of any copyrighted software for which the diocese/parish/school or the end user does not have a valid, active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and prohibited.
4. Knowingly or negligently introducing viruses, Trojans, worms, or other commands, scripts or programs intended to damage, disable, or degrade computer systems or network resources or to make unauthorized access of networks or systems.
5. Using or attempting to use administrative accounts or other network accounts without authorization.
6. Defeating or attempting to defeat content filtering systems.
7. Stealing, using or disclosing another user's password or code without authorization.
8. Using any network systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, Canon Law, or Diocesan rules and policies. This includes morally objectionable materials, files, images, text or other content.

Appendix B – Network Security Policy and Usage

9. Security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning, intrusion detection or other security scanning is expressly prohibited by anyone other than systems administrators charged with responsibility for system security.
11. Executing any form of network monitoring which will intercept data not intended for the employee's system, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, system, network or account, or disguising or attempting to disguise the identity of a host, system, account, or service on the network.
13. Interfering with or denying service to any other user (for example, denial of service attack.)
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the network.
15. Providing information about, or lists of, staff, students, or parishioners to parties outside the diocese/parish/school.
16. Use of wireless access to network resources without prior written permission of the technology administrators, principal or pastor.
17. Use of resources which are wasteful or which monopolize system resources at the expense of other users.
18. Use of peer-to-peer file sharing software to access, share or trade any files.
19. Using internet for participation in Chat rooms or other web-based forums unrelated to ministry, duties or studies.
20. Engaging in any other illegal activities.

DISCRETION

Those who minister and work in pastoral settings must take great care to be consistent in representing the worth of their character online. Clear communication and respect for boundaries is needed at any level of contact. Emails, text messages, blog postings, snap chat, Instagram, Facebook, Twitter, website comments, and YouTube videos are all public forums from which a permanent record can be obtained. As a representative of the Church, users should be diligent in avoiding situations which might be the source of scandal for themselves or others. Furthermore, those to whom we minister must be educated on the public nature of such communication. Confidential information should never be sent via email.

EMAIL, INSTANT MESSAGING, AND VIDEO CHATTING

Email and instant messaging (IM) allows for increased flexibility and immediacy in communication. When appropriately combined with face-to-face communication, email and IM can significantly enhance how we minister to others. The same boundary issues that must be respected in oral communication must be respected in written ones. Good judgment should always be used with text-based communication tools. Parental/guardian consent needs to be obtained when communicating by email or instant messaging with young people.

- Maintain a separate email account for your professional communication and only use this account when communicating with youth.
- Email, IM, and Video Chatting communication should only be used with matters that deal with an individual's professional relationship. Communicate only about matters that address the business-at-hand of your ministry.
- Care should be taken to maintain professionalism and appropriate boundaries in all communication.
- There should be absolutely no personal exchanges.
- Electronic communication can be easily misinterpreted. Communicate in person whenever possible. Before sending an email, ask yourself if someone might "read something into it" that you didn't intend. If you think your email might somehow be misunderstood, don't send it.
- If there is any potential for embarrassment or harm, reconsider sending the email or IM.
- Be cautious when sending an email, especially either in haste and/or when emotions are involved.

Always avoid any communication that might be construed as having inappropriate sexual or romantic overtones. Do not reply to any such email from a minor. Instead, make a copy of such inappropriate communication and notify your supervisor. Remember, there is no such thing as a private email. All emails and IM's can be logged, archived, and forwarded to other parties. Your communication can quickly become a public matter.

- Unlike verbal communication, any form of written communication has a form of permanence.
- There should be no expectation of privacy.
- At no time is one-on-one video chatting appropriate with young people.

MINISTRY WEB PAGES

Anyone who establishes a ministry web presence should make a commitment to this vehicle of communication. Web pages, especially the index or main page(s), should be regularly updated. As with any ministry effort, there should be an intentional plan and set of goals regarding establishing and maintaining a web presence. Great care should be used to protect people on a web page that is publicly accessible.

Appendix B – Network Security Policy and Usage

- Personal information should never be made available (i.e. home address, home or cell number, home email address, etc.).
- Written authorization must be obtained from parent/guardian before posting photos or videos of young people.
- Pictures or videos should not be captioned with a young person's name unless the parent/guardian has given you written authorization to do so.
- Never use a picture or video that might be considered embarrassing or unflattering.
- Care should be taken to protect the reputation of our church membership. If individuals are uncomfortable with a particular photo or video, it should be immediately removed from the website.

SOCIAL NETWORKING

A social network service utilizes software to build online social networks for communities of people who share interests and activities. Most services are primarily web-based and provide various ways for users to interact, such as chat, messaging, email, video or voice chat, file sharing, blogging, discussion groups, etc.

Social networking has become a part of everyday life, as a variety of social networking tools are being used by millions of people on a regular basis. The most popular sites include www.facebook.com, www.twitter.com, www.instagram.com, www.snapchat.com and www.tiktok.com. Social networking has revolutionized the way we communicate and share information with one another. Therefore, it can be a way to connect people with the church and the church's activities with people.

On any social network site, personal opinions and discussions are often conducted. It is essential for users to remember that even on the World Wide Web, others may recognize them as representing the values of the Catholic Church.

- If a professional staff minister wants to use social networking sites for ministry purposes, a professional social networking account should be created that is separate from their personal account. This account should be seen as an official extension of the ministry organization's web presence, administrated by an adult, and approved by the pastor or supervisor in which the social networking site will be used. Volunteers should not set up a special ministry site without the permission of the professional staff minister and/or the pastor.
- There is a difference between initiating a 'friend request' and accepting one. Pastoral ministers must not initiate and 'seek' friends on the professional social networking account. Outside individuals must request you as a friend first.
- Using the Internet for accessing information about the people to whom we minister is a violation of their privacy, even if that information is publicly accessible.

SOCIAL NETWORKING WITH MINORS

Anyone who ministers and works in pastoral settings with young people with a “personal” social networking site should never advertise that site nor “friend” a young person to their “personal” site. If you become aware of information that is in the public domain of such a site, you are responsible for information that must be reported if a minor has been abused or is under threat of harm.

“Best Practices”

Ideally, the professional minister, with permission from the pastor/supervisor, should create an online group on social networking sites that both young people and adults can join and interact without full access to one another’s profile.

BLOGGING

One method to develop and disseminate content is through a blog. The word “blog” is short for ‘Web log’ or ‘Web-based log.’ Those who minister and work in pastoral settings may only establish and publish through ministry-based blogs with the prior approval of their pastor or supervisor. As a representative of the Church, blogging should be conducted in a professional manner for ministry purposes only. As with any professional communication, ministry blogs should **not** be used:

- For any personal communication or agenda.
- To conduct or promote outside business activities.
- To defame or cause defamation of the character of any individual, organization or institution.
- To divulge any personal information about an individual or jeopardize their safety in any other way.

“Best Practices”

Ministry based blogs can publish information including, but not limited to:

- Fliers for upcoming activities, permission forms, calendar, and ministerial updates
- Additional links and references for faith formation
- Sacramental preparation information including: class times, checklists, sponsor resources, parent resources, etc.
- Descriptions of projects, including procedures, expectations, and suggested parent Involvement
- Bible Studies and other spiritual links and prayer resources
- Achievements of parishioners

BLOG DISCIPLINE (needs to support the student handbook)

The question that will come up frequently is “Can students with an “anti-school” message be disciplined?” The following is a recommendation that can be modified based on your student handbook.

- If the student handbook is worded so students are on notice that behavior will subject them to discipline, they can be disciplined.
- The handbook should be worded to apply to out-of-school conduct that violates school rules.
- The handbook should be worded to address behavior regardless of whether it is verbal, physical, written, graphic or electronic.
- Distinguish violation of school rules from anti-school messages.

ONLINE GAMING

Those who minister and work in pastoral settings with young people should take care in their involvement with online gaming. While this may be a recreational alternative, for many it is also an opportunity for social networking. Pastoral ministers should take care of protecting their online game identities so that appropriate boundaries are maintained.

DEFINITIONS

1. **Computer Use** — Shall mean and include the use of school computers and networks and other technology resources including, without limitation, computers and related technology equipment or networks, all forms of email or electronic communication, websites and the Internet including onsite or by dial-up or remote access thereto through school accounts, as well as any use which involves visual depictions, audio, video or text, in any form.
2. **Computer User** — Shall mean and include any parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other individuals who engage in Computer Use as defined herein.
3. **Access to the Internet** — A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet, or which accesses the Internet by dial-up or remote access using an Internet account.
4. **Minor** — Shall mean an individual who has not attained the age of 18.
5. **Obscene** — Shall have the meaning given such term in Section 1460 of Title 18, United States Code.
6. **Child Pornography** — Shall have the meaning given such term in Section 2256 of Title 18, United States Code.

Appendix B – Network Security Policy and Usage

7. **Hacking** — Shall mean Computer Use or using the Internet to attempt to gain unauthorized access to proprietary computer systems.
8. **Technology Protection Measure** — Shall mean and refer to a proxy server that blocks and/or filters Internet access.
9. **Adult** — Shall mean and refer to individual age 18 or older.

(Revised 10/2021)

PHOTOGRAPH AND VIDEO CONSENT FORM:

From time to time, pictures and video may be taken of events and gatherings. We would like to be able to use these photographs and videos for flyers, parish and arch/diocesan publications, and the ministry website. Written consent of both the student and parent/guardian is required. Names will not be posted unless written authorization is given by the student and parent/guardian, and then only first names will be used. If there are concerns about pictures or videos posted on the website, please contact the ministry coordinator or webmaster, and they will promptly be removed.

I/We, the parent(s)/guardian(s) of this youth (name) _____, authorize and give full consent, without limitation or reservation, to (parish/school) _____, to publish any photograph or video in which the above named student appears while participating in any program associated with (parish/school)_____ ministry. There will be no compensation for use of any photograph or video at the time of publication or in the future.

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Catholic Mutual...CARES

PROTECTING YOUR NETWORK FROM INTERNET/EMAIL RISKS

Loss of valuable, confidential data, downtime and damaged systems are not pleasant issues to deal with. They can cost your organization a significant amount of money, not to mention the time involved to resolve the problems. Properly securing your computer from the numerous threats posed by viruses, spyware and hackers is just as important as being aware of the Internet's dangers. A brief investment of time and effort is all that it takes to make sure that your computer remains free of malicious software and is off limits to hackers. Implementation of the following measures will go a long way to protect your local area network (LAN). All organizations should have an IT individual or staff that would be responsible for overseeing these safety measures:

- Limit floppy drive access, USB ports and serial ports on networked computers. These are the most common entry points for problems and most users do not need access to these drives. They can email or store data elsewhere in a safe "scanned" environment.
- Do not allow any users to modify any system files. All network users should be locked down so they can only perform tasks which administration has agreed upon.
- Block Instant Messenger. These send messages and attachments out to a server and then back to its clients. By disabling its functionality, viruses and other computer risks can be controlled from spreading.
- A current subscription of antivirus software should be run on all your computers. Examples of the "current" top products are made by Trend Micro, Kaspersky, and Cyber Reason.
- Install a firewall which helps prevent unauthorized sources from entering or leaving your computer, making you invisible on the Internet. A firewall should always be used if you have a broadband connection (DSL or cable). A firewall product can either be hardware or software. There certainly should be a firewall at the top of the network taking care of incoming traffic, but a good software-based firewall installed on each computer does help as well.
- Never open attachments to an email unless you trust the sender as this is often what triggers a virus to enter your computer.

Appendix C – Protecting your Network from Internet/Email Risks

- Install filters to prevent users from accessing forbidden sites. Consider using a mechanism which allows you to monitor or track an individual users' behavior on the web.
- Install a port monitor to prevent your ports from being scanned. Hackers regularly try to find and exploit weaknesses in operating systems and web browsers.
- Require passwords to be changed frequently and the password must not be the same as any of the previous six passwords. Passwords should contain both letters and numbers or symbols.
- Require the combination of keystrokes CTRL+ALT+DEL to logon. This provides an additional security layer requiring the user to physically be at the computer to log on.
- Use password-activated screen savers to lock computers after a period of inactivity.
- Continuously update your operating system and web browsers. Most can be set to check for updates automatically.
- Maintain backups of your software applications and files at a secured, off-site facility. Use encryption to protect any sensitive information.
- Enact an Email and Internet Policy. All users should be given a hard copy to read and required to sign and date they have read and understand the policy.
- Develop and implement a Security Plan and train users properly to ensure confidential information is kept secure.
- Avoid putting photos of individuals on your website, especially minors, unless photos are located under an area that is password protected.
- Ensure your IT individuals are up to date on the latest technology.

(Revised 10/2021)

Catholic Mutual...CARES

DATA PROTECTION POLICY

The Church is constantly evolving and making changes to meet the technical needs and expectations of its parishioners. Dioceses, parishes, and schools have developed their own websites and offer services online in an effort to keep up with today's society. Some of the online ventures being offered by Church websites are fundraising, chat rooms, bulletins, employment applications, online tuition/collection/donations, etc. Oftentimes, personal information is collected by the Church electronically from individuals, including names, addresses, phone numbers, bank and/or credit card account numbers, incomes, etc. A policy should be in place to properly safeguard diocesan/parish sensitive information, as well as the personal information of parishioners, students and employees. The following items should be considered when developing a policy for data protection.

- 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.
- Users should be required to utilize passwords that are at least ten characters and contain a combination of letters, numbers, and symbols. Passwords should be changed frequently.
- Password-activated screen savers should be used to lock computers after a period of inactivity.
- Procedures should be in place for the appropriate use and protection of laptops, PDA's, cell phones or other mobile devices. Any sensitive information should be in encrypted files.
- A virtual private network (VPN) should be required for any laptop, cell phone or other device accessing this information remotely.
- Employees and volunteers must be trained to ensure security, confidentiality, and integrity of sensitive information is maintained such as:
 - Locking file cabinets or doors to rooms where records are kept
 - Not allowing passwords to be shared or posted in work areas
 - Ensuring sensitive information is encrypted when sent electronically
 - Reporting suspicious attempts to obtain sensitive information to supervisors

Appendix D – Data Protection Policy

- Employees should be reminded on a regular basis of policy to keep information secure and confidential.
- Impose and follow through with strict disciplinary measures for policy violations
- Terminated employees or volunteers should have their passwords deactivated immediately
- Know where sensitive information is stored and keep it secure. Remember, only authorized individuals should have access.
 - Storage areas of sensitive paper files should be protected against damage from physical hazards such as fire or floods.
 - Sensitive records (including media such as flash drives, external hard drives and DVDs) should be stored in room or cabinet that is locked when unattended.
 - For sensitive information stored on a server or other computer, it should be password protected by a “strong” password.
 - An inventory should be maintained of all computers and other equipment on which sensitive information may be stored.
 - When transmitting credit card information or other sensitive data, use a Secure Sockets Layer (SSL) or other secure connection to ensure information is protected in transit.
 - When collecting sensitive information online directly from parishioners, make secure transmission automatic.
 - If confidential information must be transmitted by email, the data must be encrypted.
 - Servers should be physically isolated in tightly controlled and monitored facilities. Only those technical team members whose jobs require it should be able to access the server room.
 - Backup tapes should be stored in a fireproof safe in a secure, offsite location.
- Ensure disposal of sensitive information is done in a secure manner. All paper records should be shredded in a manner that it 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.



CYBER INCIDENT REPORTING

IMPORTANT: The first few minutes and hours after learning of a cyber incident are critical to a successful recovery. The following is intended to help you and your organization know how to identify and report a suspected or actual cyber security breach.

Immediately notify your IT Resource Personnel.

During business hours, contact [Jeff Schneider, Director of Claims for CMG](#):

402-514-2404 (Office) 402-490-0021 (Cell)

After hours contact our cyber insurance experts at [Tokio Marine HCC](#):

1-888-627-8995 or cpl.claims@tmhcc.com – Identify yourself as a Catholic Mutual Member

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

Cyber Event	Immediate Mitigation Steps
Ransomware infection	<ul style="list-style-type: none"> • 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 Claims
Phishing email attack	<ul style="list-style-type: none"> • 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 Claims
Malware infection	<ul style="list-style-type: none"> • 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 Claims
Discovery of unauthorized files or user accounts on server or client	<ul style="list-style-type: none"> • Close Remote Desktop Protocol (RDP) ports • Change passwords (strong and unique passphrase) • Contact CMG Claims
Lost or stolen device	<ul style="list-style-type: none"> • Report lost/stolen device to IT immediately • Secure all devices and removable media (passwords and encryption)
Mistaken wire transfer	<ul style="list-style-type: none"> • Call bank and report details • Attempt to halt transfer • Take picture/screen shot of email request of fund transfer • Contact CMG Claims

Recommended 3rd Party Vendors

The following is a list of 3rd party vendors and manufacturers that may assist with your cyber exposure.

RECOMMENDED TRAINING VENDORS

- Microsoft offers a free Internet Safety for Enterprise & Organizations toolkit. <https://www.gcflearnfree.org/internetsafety/> is a free class available for all companies.
- Lynda.com offers a series of cybersecurity awareness courses.
- KnowBe4.com is a paid service that offers Cyber Security Training and campaigns to the test user awareness through email and other media types.

RECOMMENDED FIREWALL MANUFACTURERS

Here are a few manufacturers that have content filtering, gateway anti-virus, etc. and are good for a small office environment at a reasonable price.

- SonicWALL TZ315 or newer
- Sophos XG series
- Ubiquity UniFi Gateway Pro

RECOMMENDED ANTI-VIRUS MANUFACTURERS

Use the paid versions to get support.

- Windows Defender
- Malwarebytes
- Symantec / Norton Endpoint Protection
- Bitdefender
- ESET
- Immunit
- Sophos Endpoint Protection
- Sophos InterceptX – Real-time Malware Detection
- Avira Pro – PC & MAC
- The following are not recommended for use:
- AVG Free
- Kaspersky

RECOMMENDED UPDATE SERVERS/APPLICATIONS

- Windows Update Server 3.0 (server) – Windows Patches and Updates
- Ninite Pro (application) – Third Party Updates (Adobe Reader, Chrome, Firefox, Flash, Java, etc.)
- Solar Winds Patch Manager (server) – Third Party Updates

OPERATING SYSTEMS END OF LIFE

Any operating systems that are not listed below are considered to be obsolete, are not supported, and should no longer be used.

MICROSOFT DESKTOP OPERATING SYSTEMS

- Windows 7 – Service Pack 1 – January, 14, 2020
- Windows 8 – Windows 8.1 – January 10, 2023
- Windows 10 – Version 1511 – October 10, 2017
- Windows 10 – Version 1703 – October 14, 2025
- Microsoft Server Operating Systems:
- Windows 2008 – R2 – January 14, 2020
- Windows 2012 – R2 – January, 10, 2023
- Windows 2016 – January 11, 2027

PASSWORD MANAGEMENT APPLICATIONS

- iOS, Windows, MAC, Chromium - LastPass
- iOS – oneSafe
- Windows – KeePass 2
- Mac – 1Password
- Mac – Keeper
- Mac- KeyChains

CLOUD BACKUP SERVICES

- Carbonite
- iDrive
- Crashplan
- TimeMachine

Catholic Mutual...CARES

CYBER SECURITY TIPS

Parishes, schools and other Catholic organizations may be daunted by the perceived resources it takes to secure their computer systems; however, not making cyber security a priority could be a costly decision. The National Cyber Security Alliance recommends implementing the following key security principles to provide a starting point for a comprehensive security plan.

1. **Ensure that all employees use effective passwords.** Encourage passwords that are comprised of different characters and change them every 60 to 70 days, but no longer than 90 days. Passwords should be required to include both numbers and letters.
2. **Protect your systems.** Install and use anti-virus, anti-spyware and anti-adware programs on all computers. Ensure that your computers are protected by a firewall. A firewall can be a separate appliance, built into wireless systems, or a software firewall that comes with many commercial security suites.
3. **Keep all software up-to-date.** Ensure that all computer software is up-to-date and contains the most recent patches (i.e. operations system, anti-virus, anti-spyware, anti-adware, firewall and office automation software). Most security and operating systems contain automatic updates; make sure that function is turned on and sign up for security notifications from the software company. Without these updates, your systems will not be well protected against new cyber threats.
4. **Create backups.** Make regular (daily or weekly) back-up copies of all of your important data/information. Store a secured copy away from your office location and use encryption to protect any sensitive information about your institution and parishioners.
5. **Be prepared for emergencies.** Create a contingency plan so you can recover if you experience an emergency. Include plans to continue business operations at an alternate location when necessary. Test your plan annually. Make sure to erase all data on the hard drive before recycling or throwing away a computer.
6. **Report Internet Crime.** Locate and join an organization for information sharing purposes. If you suspect fraud or criminal intent, report it to local law enforcement agencies, the Federal Bureau of Investigation, Secret Service or the State Attorney General's Office.

(Revised 11/2018)

Catholic Mutual...CARES

CYBER SECURITY BEST PRACTICES FOR WORKING REMOTELY

Advances in technology and the COVID-19 pandemic have paved the way for many workplaces to allow their employees to work completely or partially remote. Unfortunately, remote working and cybersecurity risks go hand in hand.

If you are considering allowing your employees to work remotely, it is important to adopt some basic best practices to protect your devices and business network from cyber liability. Following these guidelines can go a long way in enhancing your overall cyber security position

- **Use a VPN** – A virtual private network (VPN) improves online privacy. It encrypts all the internet traffic, making it unreadable to anyone who may intercept it. Confirm that your employees are using the VPN when working and when accessing workplace information systems.
- **Provide Laptops/Equipment for Work Use Only** – Whenever possible, only use laptops and equipment managed and protected by your workplace. This could be a large investment when developing a remote work environment but using workplace-owned equipment allows your IT department to customize firewalls, add stronger antivirus software, and automatic online backup tools built into business networks. Allowing employees to use a personal home computer could increase the risk of malware invading the computer and accessing personal and work-related information and should be discouraged.
- **Wi-Fi Connection** – Most Wi-Fi systems in homes are secure. When outside the home, (i.e., coffee shop, hotel, etc.), unsecure public wi-fi networks are prime targets for hackers to spy on internet traffic and collect confidential information. Encourage remote employees to work at home and minimize accessing the network on public wi-fi. Have your home wi-fi locked and password protected so that neighbors or other people can't access the network.
- **Choose Strong Passwords** – Using strong passwords is a simple way to prevent cybersecurity issues. Individual passwords should be established for each user. Individuals should not have the same password for work as personal accounts. Unless the employee is on a trusted device, the remember password function should be turned off when logging into the workplace information systems on a personal device.

Appendix I – Cyber Security Best Practices for Working Remotely

- **Two-factor Authentication** – Adding a second authentication process for each employee adds an extra layer of protection in preventing the risk of a leak or data breach. The extra step of requiring an email or text confirmation code to the system will reduce access to the data if it was hacked or breached.
- **Backups** – Back-up systems are important to have on employer owned equipment. The system should be backed up regularly to the Cloud. This will save time if a breach occurs. If there were a breach, all the data would be lost without a backup.
- **Install a Firewall** – A firewall is an additional line of defense to prevent data hackers/breachers from entering your system. It creates a barrier between the employee's device and the internet when closing ports to communication. Most employee's devices will have a built-in firewall and if the employee is using a router, a firewall can be enabled on that too.
- **Antivirus Software** – Antivirus software should be installed and fully updated on devices as a next line of defense if threats do get through a firewall. Advanced antivirus software can detect, and block known malware.
- **Encryption** – If employees need to send sensitive information to fellow employees or Church members, encrypted tools should be installed on their device. Many mainstream messaging services come with end-to-end encryption as a default setting or as an option. This will eliminate access by a hacker to sensitive communication. Encryption is also provided with the use of a VPN.
- **Locking Devices** – If employees are working remotely or in a public space, they should ensure that the system is locked or shut down when leaving the device. Password protection should also be in place, which would not allow access to the system until the password is entered.
- **Phishing** – Train employees on how to spot phishing attacks. Employees should be warned of suspicious emails from people they don't know – especially if they are asked to open a link or attachment. Even emails sent from people they know, but asking for unusual things, should be suspect. Every email should be read carefully. Oftentimes, emails that look legitimate may have misspelled words or phrases that can be caught if read.
- **Enable “Find My Device” and/or Remote Wipe** – If your device is lost or stolen, finding the device and securely wiping the device makes it more difficult for hackers to access the data. There are different settings for software programs/equipment that your workplace may be using to set this up.

Catholic Mutual...CARES

Electronic Signatures (e-signatures)

As technology continues to evolve and develop into our everyday lives, electronic signatures are becoming more prominent. An electronic signature or e-signature is defined as a symbol, sound, or something else in electronic form used by a signatory (signer) to represent his or her signature. If legal and/or regulated in your State, e-signatures have benefits of increased efficiency and enhanced security.

For e-signatures to be valid and legally binding, they must adhere to certain standards. In the United States, e-signatures are both legalized and regulated under two separate laws, the United States Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) which makes e-signatures valid and uniform across state lines. UETA has been passed in all 47 states, plus Washington, D.C. and the U.S. Virgin Islands. New York, Illinois and Washington have their own laws regulating e-signatures.

For an e-signature to be legitimate, it must possess the following attributes:

- 1. The signer must be aware of their actions and intent to sign.**
- 2. The signer must have given consent indicating they agreed to allow the transaction to take place electronically.**
- 3. The electronic software that captured the signature must keep a record of the process used to obtain the signature.**
- 4. The documents that were signed electronically must be retainable for recordkeeping purposes and reproducible, so all parties have a copy.**

When contemplating using e-signatures, you should ensure the four criteria listed above are met.

Should you have any additional questions, please feel free to contact your Risk Management Representative at Catholic Mutual Group.

(Revised 2/2019)

Using Video Conferencing Services Safely

The world has been moving into a more digital and online environment. This is very evident for those that work from a remote location. Remote workers have realized the importance of using video conferencing services such as Zoom, Microsoft Teams, Cisco Webex, etc. These conferencing options are key for employees and employers to communicate, collaborate and meet when working remotely.

It's important to ensure you are mindful of security when utilizing any video conferencing software. The following best practices are recommended when using a video conferencing service.

1. Only download these applications/services from the provider itself to avoid accidentally installing malware on your computer. Ensure you have the most up-to-date software.
2. Don't use the same ID for all of your meetings. Set up a unique meeting ID for every scheduled conference. Otherwise, it makes it easier for hackers to video-bomb your meetings or record them.
3. Set up a waiting room area for your video conferences. This way you can see everyone that wants to join the meeting and screen them before letting them into the conference. This is a good way to prevent video-bombers from causing a disruption to your meeting.
4. Provide a meeting link directly to those you wish to invite to the meeting. Do not send a broadcast email with the meeting link.
5. Provide a password for your video conference to help prevent unwanted attendees from crashing your meeting.
6. Make sure there is only one host for your meeting and this person is the only one that can control screen-sharing, video and mute options, record options and allow guests into the meeting.

Catholic Mutual...CARES

Electronic Fiduciary Transaction Requests

A request to conduct any online fiduciary transactions between your Arch/Diocese, parishes/schools, businesses and/or financial institutions can put your money and identity at risk. The key to safe online financial transactions is to always be informed of the everchanging cyber security environment and being cautious of new threats. When you receive a request to perform a fiduciary transaction, the following recommendations should have been instituted prior to and be performed during any wire transfer.

- If your Arch/Diocese and/or parishes utilize Microsoft Outlook for email, we recommend you implement the “2 Factor Authentication” (2FA), to add another layer of protection to password-protected remote access to your email. It is an authentication method that includes a password and time sensitive code, something only you will know.

Even if a hacker has stolen your login credentials, 2FA should prevent them from accessing your email account as the hacker would also need to have the employee’s mobile phone which is being utilized as the 2nd form of authentication. Please know, just having passwords is no longer enough to protect your email accounts. Remember, all online transactions should take place on a website whose address begins with: https://. The “s” means the site is secure. If you don’t see the “s,” do not trust the source.

- Wire Transfer Fraud is a top cyber threat to your financial accounts. Wire Transfer Fraud is when employees are deceived by criminals to wire money to a bank account controlled by them. A hacker can impersonate a bank, business (construction company), the Arch/Diocese or another parish. Every employee allowed to conduct wire transfers must be trained to be alert and always verify any changes made to the instructions of an existing wire transfer and a request to set up a new wire transfer. This verification must be conducted by calling a known and trusted phone number. Never use the contact information or phone number provided in the email request to wire transfer.

Only allow certain employees to send wire transfers. Additionally, any transfers should be verified by two individuals to help reduce the potential of falling victim to wire fraud. All locations which use wire transfers should implement a wire fraud reduction policy which defines procedures to reduce or eliminate the risk of wire fraud.

Appendix L – Electronic Fiduciary Transaction Requests

- Training of all employees is critical in reducing your exposure to cyberattacks. Employees should be trained regularly on recognizing phishing emails to protect against email fraud. Human error is the number one cause of a cyberattack. NEVER, click any links in the contact email. Call the source of the email directly (but not by using the contact information in a potential fraudulent email), and then verify the validity of the request. A best practice to consider is to have your emails identified as coming from an external source, therefore, prompting the employee to question the true origin of the email.

Recommended training should consist of the following:

- Phishing
 - Employee Mistakes
 - Spear-Phishing
 - Ransomware
 - Threats of a Data Breach
 - Malware
 - Safeguarding Information
- Your email system can be configured in such a way that it filters phishing emails from getting to your employees/staff. This filtering system can quarantine suspicious emails and scan documents before they are opened. Furthermore, an alert policy can also be developed to detect suspicious behavior. It consists of having rules and conditions in place which will then notify you when those rules are triggered. This alert policy can alert you to very important security-related issues such as a malicious URL being clicked on, an email containing Malware or phishing URL's and/or infected email messages. When considering an alert policy, it is recommended to assign a higher severity level to the aforementioned activities. Checking emails and having an alert policy in place can help identify a compromised email and expose criminal activity. As such, the configuration of your email system can flag emails with similarities of your own address.

Example: saintmarys@church.com vs. saint-marys@church.com

- Having an advanced endpoint protection system in place will also reduce your exposure to a cyberattack. Endpoint protection uses artificial intelligence, behavioral detection and machine learning algorithms to protect you and recipient of your transactions/emails. As always, once your transaction has been performed, never assume the transaction was completed safely. Always confirm with the recipient of the transaction to ensure it was submitted securely. If not, cancel the transaction immediately.
- The warning sign of wire fraud is typically an email with a request to change existing wire instructions like a bank account or mailing address. When you get an email request like this, **warning sirens should go off in your head! ALWAYS VERIFY!**

Should you need further assistance, please do not hesitate to contact your CMG Risk Management Representative at 800.228.6108.

(Rev 10/2021)

Catholic Mutual...CARES

Simple Technology Assessment and Health Check

Cyber Security Policies and Procedures:

1. Do you have a documented Cyber Security Policy?
2. Does the policy address items such as two-factor authentication, portable media, mobile devices and wireless access?
3. Are employees aware of, understand and trained to follow the policy?
4. Are the policies and procedures reviewed regularly and kept up to date?

Network and Asset Protection:

1. Do you have adequate firewalls?
2. Are applications regularly patched for updates?
3. Has your asset inventory been documented to include the equipment and who possesses the equipment?
4. Are user accounts controlled, monitored, and protected against unauthorized physical access?

Data Protection and Recovery:

1. Have you defined what types of data need to be protected and at what level?
2. Are appropriate protection and encryption technologies in place?
3. Is data regularly backed up and protected?

Anti-Malware Measures:

1. Do you have adequate anti-malware software installed on equipment?
2. Does the anti-malware software regularly scan to detect malicious files from e-mail, compromised websites and other sources?
3. Are applications regularly patched for updates?

Contingency Planning and Incident Response/Recovery:

1. Can you identify a cyber-security incident when it happens?
2. Do you have a response plan in place?
3. Have you tested recovery processes such as the restore-from-backup scenario for success?
4. Does your plan include a plan for core business activities should a major system failure occur?