Archdiocese of Omaha
INFORMATION TECHNOLOGY STANDARDS - CYBER SECURITY

Cyber Security is the responsibility of every person using computer systems at the Chancery, parishes, schools and any other diocese 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 jeopardize the parish or diocese. In addition, criminal attacks can lead to severe temporary or permanent damage to any network.

This document describes industry best practices and minimum standards for increasing security and stability of the office computer networks.

An annual review of this document is necessary as technology changes continuously and requires constant review.

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 or mobile devices 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. (See the Appendix for Recommended Training Vendors.)

Minimum standard: Employees with financial or accounting responsibilities are required to complete annual social engineering training and be included in phishing simulation campaigns every 30 – 60 days.

NETWORK/WORKSTATION DEFENSE

Internet-facing firewalls should only have incoming ports open when needed for services, such as email and/or web servers, 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 Filters, DNS filters and Botnet Filters. These features are often found in lower-end firewall manufacturers. These devices have about a 3 to 7 year life. (See the Appendix for Recommended Firewall Manufacturers).

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.

Minimum standard: All computers must have a firewall solution implemented. A network-based Internet-facing firewall must be installed and provide port/application/IP filtering, content filtering, gateway anti-virus/anti-malware, and intrusion prevention.

WI-FI

Wireless networks must be password-protected. There should be at least two SSID's associated, one for public internet access (guest networks) and one for private office access. All wireless SSID's should be WPA2 or WPA3 encrypted. Devices and associated network traffic from the guest network should be on a separate VLAN or network.

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 I.T. personnel should know it. Personally owned equipment, including all mobile devices, MUST use Guest networks.

It is further recommended that 802.1x / two-factor authentication in conjunction with Active Directory (see below) 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.

Minimum standard: If you have WI-FI all SSID's must be WPA2 or WPA3 encrypted. If an SSID is provided for public internet access (guest networks) and one for private office access. Devices and associated network traffic from the guest network should be on a separate VLAN or network.

ENDPOINT DETECTION AND RESPONSE, UPDATES AND PATCHES

An Endpoint Detection and Response (EDR) that includes centralized monitoring and logging of all endpoint activity across the organization or a Next-Generation Antivirus (NGAV) with EDR functionality must be installed on every system, whether be it Windows, Mac, or Linux. It is very important to update operating systems (See appendix Recommend Update Servers/Applications), security related software, and browsers regularly. Full scans should be done at least once per week. (See the appendix Recommended EDR and NGAV Manufacturers)

Minimum standard: All systems must have Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV)) with EDR functionality software installed.

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 and exploiting security related vulnerabilities. Centralized authentication also paves the way for the use of 802.1x-based authentication and multi-factor authentication ("MFA") for stronger protection of wireless networks and remote access to systems.

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. As of this writing, anything earlier Windows 10 is no longer supported, and Windows 10 versions prior to 2004 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 in place. (See Appendix for Operating Systems End of Life schedule).

***Current Recommendation: Windows 10 version 21H1 or greater, macOS 10.14 ("Mojave") or greater.**

PASSWORDS AND AUTHENTICATION

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 12 characters long. Do not store passwords on paper and stick 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 60 – 90 days. Avoid using the same password on different systems. Do not reuse the same password, especially for email and banking. (See the Appendix for Password Manager Applications).

Passwords in parish or school information systems such as PDS, ParishSOFT, PowerSchool or on third party software should also be changed every 90 days. Any time a service like PDS Church Office, Facebook, Office 365, Sycamore or Gmail offers a "two-step verification" or "multi-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 in the event of an attempt to access an account the attacker won't be able to sign in, even if they know your password.

Multi-factor authentication should be used for remote access to internal networks (including remote desktops), email, applications and services that contain sensitive PII information, and for wireless access to internal networks (802.1x).

Multi-factor authentication should also be used for all local and remote access to privileged user accounts.

Minimum standard: The use of multi-factor authentication to secure all remote access to your network, including any remote desktop connections, email, and all local and remote access to privileged user accounts.

PHISHING AND OTHER SCAMS

phish·ing ˈfiSHiNG/ noun

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 aren't absolutely confident that it came from a trusted source.

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.

SENSITIVE INFORMATION PROTECT

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, encrypted email or over the phone. This information in physical form, if needed, must be secured in a locked cabinet or safe when not in use. Where resting in stasis (storage) on computer systems, all such PII should be encrypted. Information on location websites should also be cleaned of email addresses and direct phone numbers. These can lead to page scraping by spammers. Consider using a single Contact us page instead that directs the request to a receptionist email or phone.

All sensitive PII and confidential information should be stored on segregated servers and users access should be provided based upon role (group) based assignments.

Use of Flocknote or other communication systems like Constant Contact or Mailchimp should replace outgoing office email messages that contain large numbers of parishioner or parents email addresses.

Minimum standard: All sensitive and confidential information stored on your organization's systems and networks must be encrypted.

EMAIL, EMAIL ADDRESSES and DOMAINS

Each location should have a domain name that is similar to the location name and easy to remember. Here are a few examples of this:

St. Vincent de Paul in Omaha https://www.svdpomaha.org/

Christ the King in Omaha https://ctkomaha.org/

Personal or generic email addresses from companies like Gmail, Yahoo, AOL, etc., should not be used for business purposes. Mixing personal and business email is never good. Also, it's much easier for your constituents to spot a phishing attempt when an email address matches your location instead of something like frgregbaxterparish@gmail.com.

The cost of setting up a domain name and email attached to it is much less than being scammed or having your reputation marred by the bad guys trying to imitate your address.

An email solution or provider should be selected that provides secure account access through multi-factor authentication and provides effective spam filtering capabilities. Additionally, email filtering designed to prevent phishing or ransomware attacks (in addition to a general spam filtering solution) is necessary.

Minimum standard: An email filtering solution designed to prevent phishing or ransomware attacks (in addition to a general spam filtering solution(s) provided by your email provider) must be in place.

Note: previous multi-factor authentication minimum standard for email access.

REMOTE DESKTOP ACCESS

There are many applications for gaining remote access to location desktops and servers. All must include the ability to do the following:

1. Blank the local screen when a remote connection is established.
2. Require a password for every logon attempt.
3. Multi Factor Authentication (MFA).

Minimum standard: All remote desktop access must require a password for every login attempt and MFA

LOCK COMPUTERS AND DEVICES

Physical access to equipment such as servers 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 information on the move.

SECURE PORTABLE MEDIA

Portable devices such as mobile phones and laptops should have limited 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 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

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, either as a dedicated cloud service or kept in a cloud syncing service, are another option to keep your data safe. They should utilize the following: restore to a point in time from multiple backups, are immutable, access protect by MFA and utilize encryption. (See Appendix for Cloud Backup Services).

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

Minimum standard: Weekly backups using a backup solution for all critical data, where the backed up data is segregated and/or disconnected from your network in such a way to reduce or eliminate the risk of the backup being compromised in a malware or ransomware attack. Kept in a dedicated cloud service protected by MFA **OR** kept in a cloud-syncing service protected my MFA; is tested semi-annually; can be used to restore essential network functions within 3 days of widespread malware or ransomware attack.

SUPPORT

Often overlooked, support may be the most critical consideration with regard to a 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. However in today's environment, having internal support may not be enough. Other considerations need to be thought out.

Nowadays, contracting with outside monitoring firms should be seriously considered part one's IT

program for not only avoiding and preventing potential cyber threats but also detecting when one might be underway. Utilizing a company that is constantly monitoring, scanning, and responding to any cyber-attack will help you identify a threat and notify you before you've been compromised. And while a service such as this might be viewed as an expense not needed, consider the following real example.

In the middle of the night, an organization's server was infiltrated and made inaccessible because a user's credential was obtained and used to login into the network. The attackers demanded a ransom in the amount of $240,000 for the code that would allow for the access to the servers. However, had there have not been a service recognizing what was happening the impact could have been much worse.

The impact of the attack cannot be underestimated. It was not just the matter of the ransom, but also the painstaking work that followed. It took months to be able to get everything back to where it was before. It created the necessity of notifying tens of thousands of individuals whose names may have been compromised, and required notification of local, state and federal agencies.

In this example, had it not been the work of the IT monitoring company to not only understand what was happening, but what to do, the damage could have been much worse. This is why it's strongly recommended that beyond hiring an individual to handle your day-to-day IT needs, you should look to utilize a company or service that can help with your monitoring.

WORK-RELATED DEVICE SOFTWARE AND SAAS POLICY

The location should have clear rules for what employees and volunteers can install, use and keep on their work-related devices. Make sure they understand and abide by these rules by limiting administrative rights on the location machines. Unknown outside programs and web-based services can open security vulnerabilities in your network. Only install or provide access to programs and web-based services evaluated and approved by the location Business Manager, Pastor, Principal or IT Director on location devices.

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 violations 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.

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. This can be the primary IT contact as well as Catholic Mutual, in addition to the Archdiocese IT Office.

Step 3. Instruct reporting personnel not to do anything until appropriate counsel is obtained.

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 were included (e.g. name, age, DOB, SSN, medical information); and,

Step 6. Preserve and protect the evidence.

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 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 or addressing.

Appendixes:

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 available at a reasonable price.

Fortinet FortiGate
Sophos XG series
Cisco Firepower
Palo Alto Networks NGFW Series

RECOMMENDED EDR MANUFACTURERS
Carbon Black
BlackBerry
Sophos InerceptX
FireEye Endpoint Security
Fortinet FortiEDR
Cisco Secure Endpoints

RECOMMENDED UPDATE SERVERS/APPLICATIONS

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

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

CLOUD BACKUP SERVICES
Druva
Veam
Carbonite
Rubrik

iDrive
TimeMachine

OPERATING SYSTEMS END OF LIFE

Any Windows operating systems not listed below are obsolete and are not

supported. Microsoft Desktop Operating Systems:
Windows 8 – Windows 8.1 – January 10, 2023
Windows 10 – Version 1809 – November 10, 2020
Windows 10 – Version 1903 – December 8, 2020
Windows 10 – Version 1909 –May 11, 2021
Windows 10 – Version 2004– December 14, 2021
Windows 10 – Version 20H2– May 10, 2022
Windows 10 – Version 21H1– December13, 2022

Microsoft Server Operating Systems:
Windows 2012 – January, 10, 2023
Windows 2012 – R2 – January, 10, 2023
Windows 2016 – January 12, 2027
Windows 2019—January, 9, 2029