DIOCESE of AUSTIN

Version 1.0 – FY23

# Information Technology Infrastructure Baseline Requirements

Cybersecurity has become vital to protect all diocesan entities, its employees, our parishioners, and our students. It is the responsibility of us all to adhere to standard security procedures to prevent the loss or theft of parishioner, student, donor, or employee confidential information.

The purpose of this document is to establish baseline requirements for facility information technology that will ensure the security and stability of the office computer networks. These baseline requirements are based on established best practices and items required to maintain our cybersecurity insurance coverage.

A regular review of this document is necessary as technology changes continuously. The document is divided into topics. In each topic, baseline requirements are established and additional recommendations are outlined. The expectation is that all entities must meet all the baseline requirements, at minimum, and put in place as many of the recommended items as feasible.

At the end of the document is a Checklist that must be completed.

## Workstations (Laptop/Desktop Computers) and Servers

### Operating System

**Baseline Requirement** – All workstations and servers must run a current, supported, Operating System.

All major computer operating system vendors have different versions of their products. These are usually divided into major releases (Windows 7, Windows 10, macOS X, macOS 11, etc.) and maintenance updates. Normally when a new major release comes out, the prior version will continue to be supported for a set period. For instance, Windows 10 was released in 2015, but Microsoft continued

to support Windows 7 until 2020. Once that time is up, there is no longer development on that release, so should a vulnerability be found, the company is not obligated to fix it. This means that running an operating system that has gone past its "end of life" is a security risk.

**Current Operating Systems as of this posting (October 2021):**

> Microsoft: Windows 10 (Version 2004, 20H2, 21H1), Windows 11 (available soon), Windows Server (2012, 2012R2, 2016, 2019, 2022)
>
> Apple: macOS 10.14 (Mojave), macOS 10.15 (Catalina), macOS 11 (Big Sur), macOS 12 (Monterey)
>
> Other Server Operating Systems (Linux, Unix, etc.): Verify with manufacturer

How to update your computer to the latest version of the operating system (Workstation):
*Note: Version updates to the OS are complementary. Upgrading to the next major release may incur a charge (e.g., upgrading from Windows 10 to Windows 11)*

> Windows 10*:* **Start > Settings > Update & Security > Windows Update**, and then select **Check for updates**. If the latest version is not available via Windows Update, then you can install it manually via the Update Assistant - Windows 10 Update Assistant (microsoft.com)
>
> Apple: Update macOS on Mac - Apple Support

**Baseline Requirement –** All Operating Systems (OS) must be patched regularly.

In addition to running a current, supported, operating system, it should be updated regularly. The OS vendors are constantly releasing security and functionality updates for their respective OS. These are often to fix a potential security issue that was discovered in the OS. It is imperative that you update regularly to ensure your system is protected from these vulnerabilities.

It is highly recommended that you set all workstations to automatically update at a set time, usually afterhours. However, be sure that the systems are powered on during this window otherwise the updates will not run.

> Windows: **Start > Settings > Update & Security > Windows Update**, and then select **Check for updates**.
>
> Apple: Update macOS on Mac - Apple Support

## Endpoint Protection

**Baseline Requirement** – Endpoint Protection w/ EDR installed on all workstations and servers and updated regularly.

Endpoint Protection, commonly referred to as Anti-Virus software, is required on all user computers including both desktops and laptops. In addition to standard Anti-Virus protection, the Anti-Virus

software must include EDR (Endpoint Detection and Response) capabilities. This goes beyond simple virus detection and removal and adds the ability to quickly detect infection and stop the propagation of any detected infection.

There are many companies that provide endpoint protection with EDR, but the diocese has partnered with Sophos and use their Intercept X w/ XDR product to meet this requirement.

**Recommended Upgrade –** Many providers offer a third-party monitored version of the product. Sophos calls it MTR for Managed Threat Response. This is a viable upgrade if you want to take a hands-off approach to monitoring your systems.

## Device Encryption

**Baseline Requirement** – All workstations (desktops/laptops) must utilize hard drive encryption.

Device encryption is the process of scrambling data into illegible code and making it indecipherable to anyone without a password or a recovery key. The data is encoded using an encryption algorithm to turn it into an unreadable format. This makes it impossible for data to be gathered from a lost or stolen computer.

Both Microsoft Windows (BitLocker) and Apple macOS (FileVault) include drive encryption for free.

More information on Microsoft BitLocker can be found at - https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

Information on FileVault for macOS can be found at - https://support.apple.com/guide/mac-help/encrypt-mac-data-with-filevault-mh11785/mac

**Baseline Requirement** – Removeable media must utilize device encryption.

Removeable Media such as USB Flash Drives, External Hard drives, etc. should also be encrypted. These devices are even easier to be lost or stolen so device encryption is vital to keep data safe.

Just like with Hard Drive encryption, the built-in tools in Windows and macOS can be used to encrypt removable media as well.

Windows 10 – Follow the section “Turn on standard BitLocker encryption” in the following article and select your removeable media. https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

macOS – Follow the instructions in the following article - https://support.apple.com/guide/disk-utility/encrypt-protect-a-storage-device-password-dskutl35612/mac

There are also various third-party software options that will encrypt your devices such as Veracrypt. It is recommended that you utilize either the built-in Operating System tools or use a paid software such as Veracrypt. Avoid any freeware as sometimes the provenance of these tools is suspect.

## System Backups

**Baseline Requirement** – All Servers must be backed up regularly, and backups must be encrypted.

Automate server backups and schedule them to run at regular intervals (daily backups recommended). It is suggested you use the 3-2-1 method and create 3 copies of each file on 2 different media (SSD/Disk, Disk/Tape or Disk/Cloud) and 1 copy kept offsite. Logs should be checked regularly to ensure backups are running and completing.

**Recommended Upgrade –** It is highly recommended that you airgap one copy of the data. Air-gapping means this copy of data is offline and is inaccessible should your network be compromised. This can be done via a cloud service or by saving a copy to tape.

**Baseline Requirement –** Test backups regularly.

Perform both file level and full system restores on a scheduled basis to confirm backup jobs are running correctly and you will be able to recover data whenever necessary

## Screen Lock

**Baseline Requirement** – All workstations should be set to automatically lock after 5-15 minutes of inactivity.

Locking your computer when you walk away from your desk is the easiest way to protect your data. If you leave your computer unattended and unlocked, someone could sit at your desk and have full access to everything you do.

## Software

**Baseline Requirement** – All software installed on workstations is reviewed and approved by the Parish/School and is regularly updated.

Any software that is installed on a user's workstation should be reviewed by the Parish/School IT personnel (or Diocese IT) to ensure it is safe to use and there are no conflicts with other programs. Freeware, Shareware and software with questionable provenance should be avoided. Browser plug-ins like search tools and coupon printers should also be avoided as these often contain malware.

All additional software should be patched/updated regularly just like the operating system.

# Printers

**Baseline Requirement –** All printers with network capability (wired and/or wireless) should be secured to avoid unauthorized access.

Any printer/copier/scan device that is network capable should have security measures in place to prevent unauthorized access. If a printer has a web management interface, a strong password should be set (different from the default device password from the manufacturer) and any unused protocols disabled. Printers that have capability such as Wi-Fi connectivity should have those features disabled if they are not being used. Network connected printers should be connected to the internal network, behind the firewall to prevent access from outside the network.

# Email

**Baseline Requirement** – All locations should utilize an enterprise grade email system such as Microsoft 365, Microsoft Exchange, Google Workspace, etc. with the following filtering and response systems in place:

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

An enterprise grade email system provides security and manageability that the personal email systems do not. This allows continuity regardless of employee turnover and the ability to create groups, shared mailboxes, etc. Personal email (Gmail, Yahoo, Hotmail, etc.) **must not** be used for official business.

**Highly Recommended** – Advanced email protection add-ons such as Microsoft 365 Advanced Threat Protection and Data Loss Prevention, or Google Workspace Advanced Protection Program

# User Accounts

## Passwords

**Baseline Requirement** – User passwords should be a minimum length of 8 characters (11 – 18+ characters preferred) with 3 of the following 4 complexity requirements; lowercase letters, uppercase letters, numbers and special characters.

Strong passwords are the first line of defense against a bad actor compromising your account. Password length and complexity is vital as this makes it far more difficult to brute force hack your account. Studies

have shown that a password of 7 characters with 3 complexity requirements (Numbers, Upper and Lowercase letters) can be breached in as little as a minute. If you increase the length to 10 characters, the time to hack the password jumps to 7 months. At 13 characters, the time to hack is 100,000 years!

An easy way to meet these length requirements is to use a passphrase. Add in a number and some special characters and you have a very strong password.

Example: *Hooray4Summer!* -or- *ThisIs1ComplexP@ssword*

Best practice would be to use a password manager such as LastPass or Dashlane. Create a complex password to access the manager, then have the manager set an ultra-complex, and unique, password for each service.

**Baseline Requirement** – User passwords must be changed at regular intervals

The length of the interval will be determined by your password complexity requirement. The longer and more complex the password, the longer the interval can be. For example, a 7-8 character password should be changed every 90 days. However, a 10+ character password can be changed after 6 months or more.

**Recommended** - Utilize Identity Access Management (IAM)/Privileged Account Management (PAM) systems.

## Multi-Factor Authentication

**Baseline Requirement** – Any account that has Administrator level access must have Multi-Factor Authentication enabled. MFA should also be enabled for user account access (Microsoft 365, Google, etc.)

Multi-Factor Authentication (MFA), sometimes called Two-Factor Authentication (2FA), is a method of confirming identity by a secondary means. Usually by sending an authentication code via text (or call) to your cell phone, via email, or via an authenticator app.

**Highly Recommended (Future Requirement)** – enable MFA on all accounts for all applications

MFA for everyone will most likely be a requirement in the future. MFA should be enabled for all user accounts on any application that supports it.

## Training

**Baseline Requirement** – All employees must attend security awareness training

The Diocese, in partnership with our Cybersecurity Insurance provider, will provide online Cybersecurity Awareness training. **All employees must** take this training at least once, usually as a new hire.

Supplemental training may be required as time goes on. For example, all employees will be required to take a training course in FY22 as a condition of our cyber insurance coverage. Information will be provided on how to access this training.

# Network

## Wired Network

**Baseline Requirement** – All networking devices (firewalls, switches, etc.) should be patched regularly

Much like computer operating systems, network hardware vendors frequently release updated firmware for their devices. By keeping your networking equipment up to date, you help protect yourself from hardware vulnerabilities.

**Baseline Requirement** – Virtual Private Networking (VPN) is required to access your on-premises systems remotely.

If you have on-premises resources (file server, etc.) that you need to access remotely, you must have a VPN in place to provide an encrypted tunnel to these resources. Non-secure inbound connection methods, such as Remote Desktop Protocol (RDP), must not be enabled across the WAN (wide area network).

**Baseline Requirement** – If you keep data on premise (e.g., local files on computers or a server) you must have a firewall in place. This should be a Next Generation Firewall with Intrusion Detection/Intrusion Prevention (IDS/IPS) capability. This also must be kept up to date and patched regularly.

A next-generation firewall with IDS/IPS functionality is another line of defense at the perimeter of your network. This helps prevent attackers from gaining unfettered access to your network.

As a bonus, most Next-Generation Firewalls can also provide VPN and Content Filtering services as well.

**Baseline Requirement** – Remote Desktop Access must not be accessible via the internet, only internally and via a VPN.

All remote applications must do the following:

- Blank the screen when a remote connection is established.
- Require a password for every login attempt.
- Support multi-factor authentication.

Microsoft Remote Desktop Protocol (RDP) is a non-encrypted protocol and can open your system up to hacking if available via the internet. If you need to access a system remotely via RDP, a VPN must be utilized to encrypt the traffic. If you use a third-party remote access system, make sure it is encrypted,

password protected and allows for multi-factor authentication. These services must also be approved by the parish/school or Diocese IT departments.

**Highly Recommended** (required for Schools) – Content Filtering

Content filtering is a method of preventing users from accessing certain resources on the internet that are determined to be inappropriate or detrimental to the organization. This can include pornography, firearms, streaming or file sharing sites, etc. Content filtering is required for our schools and highly encouraged for all other organizations.

Most firewalls provide some sort of content filtering, or you can use a service such as OpenDNS.

**Baseline Requirement** – Network Segmentation/Segregation

The network should be segmented in a way that prevents unnecessary access to privileged data. For example, Guest and IoT devices should be on separate subnets from the production network.

## Wi-Fi Network

**Baseline Requirement** – You must have at least two SSID's (networks) if you intend to provide wi-fi for guests. One SSID for public internet access only (e.g., Guest Network) and the other for your internal production network. Schools may want to add a third SSID/network for student devices.

You must use at least WPA2-Personal encryption; WPA2-Enterprise with 802.1x authentication is recommended on the internal production network. Only parish/school owned resources should be allowed to connect to this network. If you are not using 802.1x, do not give out the pre-shared key. Preconfigure systems with this information or have users come in so you can configure the system to access the network.

The Guest Network must allow only access to the internet, not to the internal network. You must also utilize device isolation, so devices on this network cannot see each other. If the Guest Network is open (i.e. no password, NOT RECOMMENDED) then you must have a Terms and Conditions splash page.

Personal devices (smartphones, tablets, etc.) are only permitted on the Guest SSID.

## Miscellaneous

**Baseline Requirement** – Meeting Applications must meet the following standards

- Require a password to join the meeting
- Host should be the first attendee

- Waiting room must be utilized and attendees must be admitted manually. Do not setup the meeting to allow bypassing of the lobby/waiting room.
- File Transfer capabilities should be set to "off" by default. Host can enable if necessary for the meeting.
- Only hosts and co-hosts should share their screens.

**Baseline Requirement** – Any cloud storage application must be approved by the Parish/School. Personal Dropbox, iCloud, OneDrive, etc. accounts should not be used for Parish/School data.

Files utilized by a group or team should be stored in Microsoft Teams/Google Drive or another collaborative cloud storage application. These files should not be stored in a user's cloud storage due to issues with accessibility should they leave the organization.

Be cautions when and with whom you share files/folders. Set expirations on all shared items.

**Highly Recommended** – Vulnerability Scans

It is highly recommended that you partner with a third-party provider for a network vulnerability scan. This process will test your network security configuration to identify any vulnerabilities. You can then make a plan to address anything found in the scan. These should be conducted yearly to every couple of years.

**Highly Recommended** – Security Incident Event Management (SIEM) software

SIEMs consolidate logs from all your network devices into a single console. You can then run reports, set alerts, etc. This software can assist with baselining network activity then make it easier to spot anomalies such as compromised accounts and intrusions.

**Highly Recommended** – Develop and test the following plans:

Incident Response/Ransomware Plan

An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work.

Disaster Recovery/Business Continuity Plan

A disaster recovery (DR) plan is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, so an organization will continue to operate – or quickly resume key operations.

---End of Document ---

Version 1.0 – Fiscal Year 2023 – November 1, 2021