GUIDELINES FOR MINIMUM-SECURITY STANDARDS FOR PARISHES AND SCHOOLS OF THE ARCHDIOCESE

POLICY

Compliance with these Minimum-Security Standards (MSS) protects not only the individual device, but also other devices connected to an Archdiocese of Miami (ADOM) network and/or cloud services. The standard is intended to help prevent exploitation of information and resources by unauthorized individuals. No system is 100% secure. The goal of these minimum standards is to build levels of protection making it more difficult for a threat actor to gain access to or compromise a system(s).

I. INTRODUCTION

A. Overview

All ADOM IT Resources and all devices, independent of their location or ownership, when connected to an ADOM network, or when storing, processing, or accessing Information hosted at any location, must comply with the MSS requirements below. Devices that do not meet these standards shall be disconnected from the ADOM or ADOM affiliated network and/or hosted services. Implementation guidelines that provide more information about complying with the minimum-security standards are linked to the individual requirements.

Devices that handle Protected Data or require a high level of Availability are required to conform to more rigorous security standards.

These guidelines should be implemented no later than December 31st, 2025. Any questions on the guidelines please contact Abel Barrera (abarrera@theadom.org, 305-986-4901).

UPON DISCOVERY OF AN SECURITY BREACH/INCIDENT:

ADOM entities will contact Abel Barrera, IT Director for the Archdiocese of Miami (abarrera@theadom.org, 305-986-4901) and Sister Elizabeth Worley, COO for the Archdiocese of Miami (eworley@theadom.org, 305-450-6420) to discuss escalation of the incident and advise on assistance needed.

B. Scope

This standard applies to all ADOM Resources and all devices, independent of their location or ownership, when connected to an ADOM and/or ADOM affiliated entity network, or when storing, processing, or accessing *ADOM* information hosted at any location. ADOM refers to any entity associated under the Archdiocese of Miami umbrella such as parishes, schools, charities, etc...

Non-networked devices should meet the MSS requirements as applicable, e.g. device lockout, passphrase requirements, use of authentication, etc.

Any guest Wi-Fi network, which is separate and segmented from the main network, is not considered an ADOM network for the purposes of this standard.

C. Exceptions

An exception is required for any configurations that do not comply with the MSS.

Non-compliant systems that do not obtain exception approval may face removal from the associated ADOM network and/or other take-down action. Departments, Units, or individuals with devices that cannot meet the requirements of the MSS may request an exception to this Standard. Approval is based on whether the risks associated with non-compliance have been adequately mitigated. All exceptions are temporary and must be replaced with compliant solutions.

Contact the appropriate IT personnel for exception requests.

II. Minimum Security Standards (MSS) Requirements

A. Patching and Updates

1. Devices connected to an ADOM network, including personal devices, must only run supported software and operating systems for which security patches are made available in a timely fashion. All currently available security patches must be applied on a schedule appropriate to the severity of the risk they mitigate.
2. Where extended vendor support is unavailable for software or operating systems deemed, “end-of-life”, an exception must be requested.

B. Anti-malware Software

When built-in anti-malware features are available in operating systems, such as with current versions of Windows and macOS, they must be enabled. Otherwise, separate anti-malware software that supports real-time scanning is required, including for network storage appliances. Windows Defender, Malwarebytes, AVG, Norton are examples of suitable anti-malware/anti-virus software.

C. Host-based Firewall Software

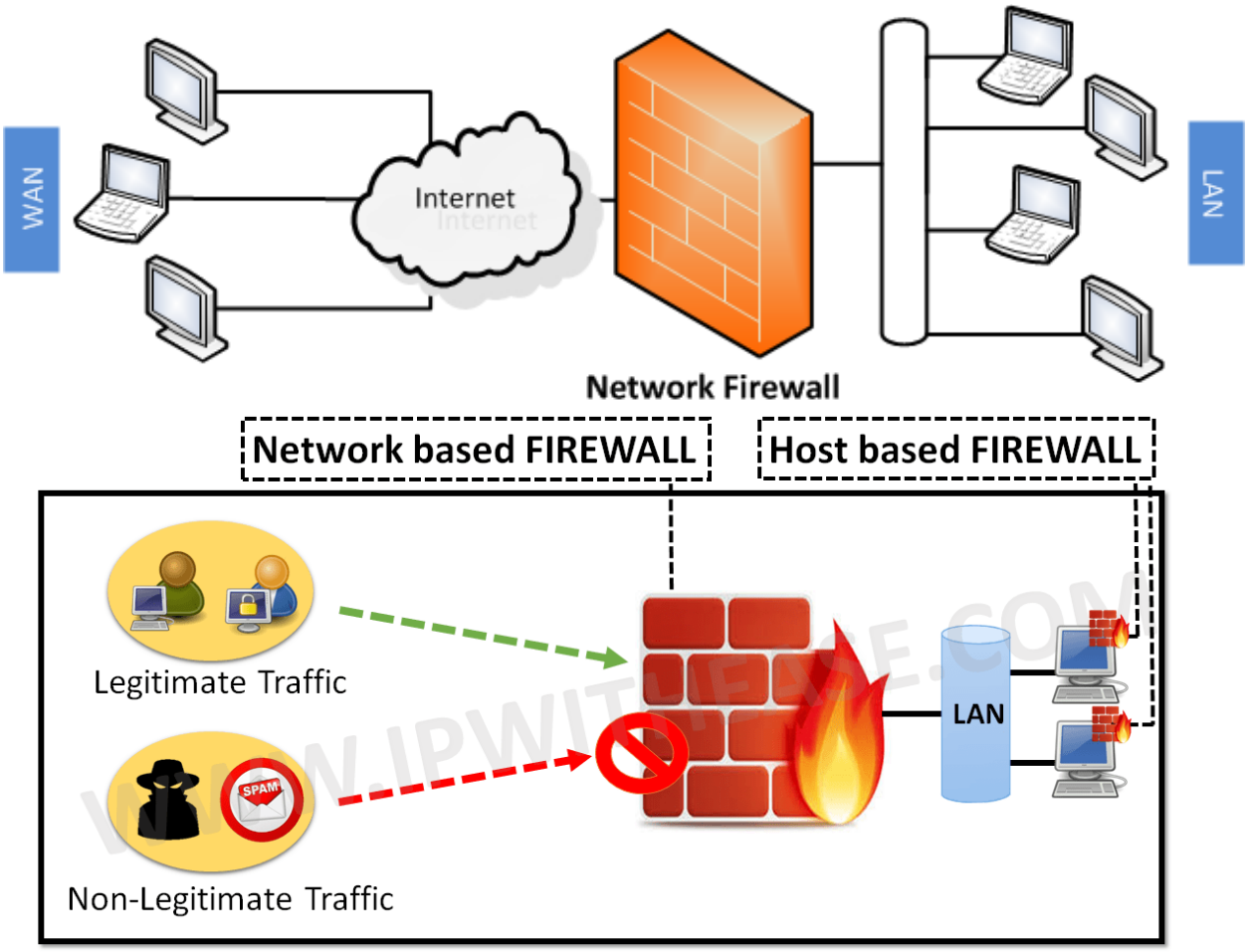
A host-based firewall is a software-based firewall that resides on an individual’s computer or device. It is designed to block incoming unauthorized ports that can be used to compromise a system.

1. Network attached systems must, wherever possible, utilize host-based firewalls. These controls must be enabled and configured to block all inbound traffic that is not explicitly required for the intended use of the device. Use of a network-based firewall does not obviate the need for host-based firewalls.
2. Microsoft Windows, macOS, and Linux/Unix devices are all equipped with firewalls though they may not have them enabled by default.
3. Many printers and network attached equipment have access controls to restrict connections to a limited number of hosts or networks in compliance with this policy. Where available, these must be enabled.

D. Network-based Firewall –

A network-based firewall is a hardware-based firewall that resides on the network in between the local area network (internal network) and the internet (wide area network WAN). It is designed to block incoming unauthorized ports that can be used to compromise a network and/or system.

Network attached systems must utilize a network-based firewall. These controls must be enabled and configured to block all inbound traffic that is not explicitly required for the intended use of the device.



E. Wireless Access

1. Wireless access points must require industry-standard, strong encryption to connect (such as WPA2, WPA3). Older encryption standards such as WEP or MAC address restrictions do not meet this requirement.
2. Management of wireless controllers and/or wireless access points must require a complex password.
3. For CLI management purposes, only SSH should be used to access network devices. Telnet is not secure and should be disabled.

F. Password Requirements

1. When passwords are used, they must meet or exceed the following complexity specifications:
2. Passwords MUST contain eight (8) characters or more following this sliding scale:
   - Complex password - 8-11 characters: mixed case letters, numbers and symbols (e.g., !@#$%^&*()_+|~-=\'{}[]:";'<>?,./'space');
   - 12 password history

3. The same or substantively similar passwords must not be used across multiple accounts.
4. PINs for mobile devices must be at least 6 characters in length. Authentication using the integrated biometric capabilities of supported devices from major vendors is also acceptable.
5. Multi-user systems must be configured to enforce these complexity requirements where technically possible.
6. All pre-assigned passwords must be changed at the time of the initial login. Multi-user systems must be configured to enforce this requirement.
7. Default and blank passwords are prohibited and must be changed to a password that meets the requirements in this Standard. If an account has a default or blank password that cannot be changed, that account must be disabled.
8. Individuals must not share user account passwords, PINs, devices used to authenticate the user (e.g., mobile phones) or tokens (e.g. multifactor tokens, smartcards, etc.) with others.
9. Passwords must be changed immediately if independently discovered, publicly disclosed, a suspected compromise has occurred, or a device on which they were used or stored has been lost or stolen. This includes the discovery of hashed (encrypted) passwords.
10. Device and account credentials such as passwords, PINs, or account recovery questions & answers must never be stored in plain text. Application secrets such as database credentials and API keys should be protected according to industry best practices.
11. Passwords should not be stored in a document on the device. Ex. a word document containing username and password with the filename password.
12. Biometrics, such as fingerprints and facial recognition, can be used in addition to complex passwords but this does not negate or supersede the password requirements listed above.

G. Device Lock-Out

1. Devices must be configured to "lock" or log out and require a user to re-authenticate with a strong passphrase/PIN, smart card or biometric lock if left unattended for more than 15 minutes, except in the following cases:
2. Devices that do not support a configuration that automatically locks or logs off users after a specified period of time (such as network appliances and consumer electronics) may meet this standard through alternate controls, such as physical access restrictions (e.g., device stored in a locked office not accessible by unauthorized users).

H. Unnecessary Services and Ports

Only network services, ports, and protocols necessary for the intended purpose or operation of a device may be running. All others must be disabled or removed.

I. Remote Access Services

1. Remote desktop, interactive shell, or terminal-level access that allows broad access from the public Internet to a system must be restricted. Indirect access using a gateway or proxy service is allowed. Only remote access services, such as proxy servers and VPN gateways, whose configuration and use have been approved by the IT Department, are allowed.
2. Remote access software such as TeamViewer, Anydesk, etc... must use 2FA or MFA, and have their passwords changed every 30 days. In addition, a tertiary password should be used to access each computer if available.

J. Privileged Accounts

1. Devices must be configured with separate accounts for privileged (administrator) and non-privileged (user) access.
2. Non-privileged user accounts must be used and only elevated to root or Administrator when necessary. A secure mechanism to escalate privileges (e.g., via User Account Control or via sudo) with a standard account is acceptable to meet this requirement.
3. Privileged and super-user accounts (Administrators, root, etc.) must not be used for non-administrator activities.
4. Built-in local Administrator accounts must be disabled.
5. Network services must run under accounts assigned the minimum necessary privileges.
6. **For devices that do not support separation of privileges:** Devices that do not provide separate facilities for privileged and unprivileged access (e.g., some network appliances and printers with embedded operating systems) are exempt from this requirement, provided they do not handle protected/sensitive data and/or on a network containing protected/sensitive data.

K. Backups

1. Data backups must be performed on a daily basis.
2. Backups must have a version history allowing restoration of data from different dates/times.
3. Data backups must be periodically tested for validity and should be stored offline so the Operating System cannot modify them. Offline refers to storage that is not located on the machine being backed up.
4. Offline backups must also be stored offsite. Offsite referring to a different location than where the devices are physically located. By storing information offsite, it protects the information from physical theft and/or a disaster such as a storm/hurricane.
5. Backups of Restricted Use data must use a solution that provides encryption in transit and at rest.
6. If a computer or device is not being backed up at night, the computer/device must be powered off.
7. Do not hoard data. Old data must be archived and removed from the server/computers. For legal purposes, old, archived data must be accessible when needed but does not need to reside on production servers. By moving old data off the servers/computers, this reduces the impact of a security breach. If the data is not accessible to the threat actor, they cannot steal and/or encrypt the data.

L. Encryption

Encryption ciphers must meet or exceed AES standards.

M. Laptops

1. Laptops must be configured to "lock" or log out and require a user to re-authenticate with a strong passphrase/PIN, smart card or biometric lock if left unattended for more than 15 minutes.
2. Laptops must have their operating system and files encrypted with applications such as BitLocker, to prevent unauthorized access.

N. Desktops

Desktops must be configured to "lock" or log out and require a user to re-authenticate with a strong password, smart card or biometric lock if left unattended for more than 15 minutes.

O. Mobile Devices

1. Mobile devices such as phones, tablets, etc... must be configured to "lock" or log out and require a user to re-authenticate with a strong passphrase/PIN, smart card or biometric lock if left unattended for more than 5 minutes.
2. Users may not install apps from unknown sources.
3. Devices must not be jailbroken or rooted. Jailbreaking and/or rooting is the process by which a devices software is modified to allow unauthorized programs to run.
4. Mobile devices, whether parish/school owned or personal, must not connect to production / internal network. Mobile devices are not as secure as computers and should be kept separate from the production network to mitigate the risk of security incidents.
5. Mobile devices must only connect to the organization's guest network.
6. Mobile devices must not connect to unprotected networks, such as Starbucks, McDonalds, Airports, etc. Unprotected/open networks such as those listed above, can have threat actors scanning them in an effort to infect connected devices.

P. Networks

1. Network services and local (console) device access must require authentication by means of passphrases or other secure authentication mechanisms (e.g. biometrics).
2. Complex passwords are required for the management of network equipment. Switches, routers, firewalls, access points, controllers, etc.
3. Networks must be segmented, to isolate parts of the network.
4. ADOM entities must have a separate guest network for mobile devices and/or non-ADOM devices.
5. For CLI management purposes, only SSH must be used to access network devices. Telnet is not secure and should be disabled.
6. All network-based authentication must be encrypted in transit using industry-standard, strong encryption mechanisms. Unencrypted services such as HTTP, Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents if authentication, confidentiality, or integrity are required.

Q. Servers

1. Local Administrator account must be disabled.

2. When a local administrator account is required, the account must be renamed and not have administrator or a variant of that name. Account must also have a complex password that is periodically changed.
3. Complex passwords must be used to access the server.
4. Unnecessary services and features must be removed.
5. Unnecessary ports must be blocked and/or removed.
6. Servers must be configured to "lock" or log out and require a user to re-authenticate with a strong passphrase/PIN, smart card or biometric lock if left unattended for more than 15 minutes.

R. Virtual Environments

1. ISCSI and vMotion networks must be segmented from data network.
2. Management networks must be segmented from data network.
3. Complex passwords are required for access to physical hosts and virtual machine management.
4. For CLI management purposes, only SSH should be used to access network devices. Telnet is not secure and should be disabled.

S. Web Browsers

1. Web browsers must be updated with the latest security updates.
2. Website passwords must not be stored on the browser.

T. Emails

1. Users should have training on spam/scam emails and should be instructed to not open attachments or links from unknown senders.
2. 2FA (2 factor authentication) or MFA (Multi-Factor Authentication) must be used to access the organization's email accounts.
3. All emails originating from outside the organization must have an "External email disclaimer" stating that the email originates from outside the organization, and not to click on links or attachments from unknown senders. ex. [CAUTION: This email originated from outside the organization. DO NOT click on links or open attachments unless you recognize the sender and know the content is safe. NOTE: Certain requested transactions require verbal and/or video confirmation.]

U. Documentation

1. Software used on the various systems must be inventoried and documented.
2. Types of data housed in the environment/network must be inventoried and documented.
3. Any changes made to the network infrastructure, servers, and/or software must be documented

V. End of Life Software and Hardware

1. Software and Hardware that are "end of life" (will no longer be supported by the manufacturer), must be upgraded to continue receiving security updates. i.e. Windows 10 will be end of life on October 14, 2025.
2. Devices such as iPads and Chromebooks must have the latest software installed.

III. Definitions

- MSS – Minimum Security Standards – minimum standards for ADOM networks.

- ADOM – Archdiocese of Miami.
- http – Hyper Text Transfer Protocol – a protocol used by internet browsers to transfer information.
- https - Hypertext Transfer Protocol Secure – a secure version of http.
- End of life – system of software that the manufacture no longer supports and/or no longer provides security updates for.
- Ports - is a unique number assigned to a connection endpoint. Ports are used to direct data to a specific software/service.
- LAN – Local Area Network – a group of devices connected to form an internal network in a local area such as an office or home. LANs are typically, behind a router and/or firewall.
- WAN – Wide Area Network – a group of computers connected to form a wide area network. WANs usually encompass computers connected over vast distances. The internet is a type of WAN network but not the only type.
- Protected Data – information/data that is not meant to be public. Information/data that requires protection. i.e. social security numbers, credit card numbers, drivers license information, personal information, etc.
- Biometrics – an authentication system that uses a person's physical characteristics to identify and grant access to a system. i.e. fingerprints, face recognition, etc.
- Sudo – superuser command in Linux software systems. Used to elevate a person's access to a specific system.
- API – Application Programming Interface – a set of rules or protocols that allow an application/software to communicate with different application/software.
- SSH – Secure Shell Protocol – A network protocol used to send encrypted communications over a network. typically used to configure/program devices.
- telnet - A network protocol used to send unencrypted communications over a network. typically used to configure/program devices.
- AES - Advanced Encryption Standard – a type of encryption algorithm used to encrypt and protect data. This standard is currently considered secure.
- WEP - Wired equivalent privacy - is an old type of wireless security algorithm designed to encrypt and protect data transmitted over a secure network. This algorithm is no longer considered secure.
- WPA - Wi-Fi Protected Access - is an old type of wireless security algorithm designed to encrypt and protect data transmitted over a secure network. This algorithm is no longer considered secure.
- WPA2 - Wi-Fi Protected Access 2 - is an old type of wireless security algorithm designed to encrypt and protect data transmitted over a secure network. This algorithm is currently considered secure.
- WPA3 - Wi-Fi Protected Access 3 - is an old type of wireless security algorithm designed to encrypt and protect data transmitted over a secure network. This algorithm is currently considered secure.
- FTP – File Transfer Protocol – a non-secure protocol used to transfer files from one device to another.
- SNMP - Simple Network Management Protocol – a protocol used to monitor devices on a network.

- POP3 - Post Office Protocol Version 3 - is a protocol used by email clients to access email messages from an e-mail server.
- IMAP - Internet Message Access Protocol - is a protocol used by email clients to access email messages from an e-mail server.
- 2FA – 2 Factor Authentication - security method that requires two forms of identification to access resources and/or data. Typically, a system that requires a phone text message with a code to gain access to a resource/data.
- MFA – Multifactor authentication - security method that requires two or more forms of identification to access resources and/or data. Typically, a system that requires a phone text message, authenticator app, or a phone call, to gain access to a resource/data.
- Host -based firewall - a software that works on a single device, providing a protection layer by examining incoming and outgoing traffic. i.e. windows firewall.
- Network based firewall - a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules.
- Malware - malicious software, developed by cybercriminals to steal data and damage or destroy computers and computer systems.
- Anti-virus - software designed to safeguard computers and/or mobile devices from malware, and cybercriminals.
- MAC - medium access control address - is a unique identifier assigned to a network interface controller (NIC), a network card. A network card/NIC is a piece of hardware used by one computer to communicate with another over a network.
- Threat Actor – a cybercriminal or hacker whose goal is to steal data and damage or destroy computers and computer systems.
- Privileged accounts – accounts that have administrative access to certain systems.
- CLI – Command line Interface – a text-based interface that allows programming of devices.
- ISCSI - Internet Small Computer Systems Interface – a protocol used for linking data storage facilities and devices. Typically found in virtual computing environments.
- VMotion – a protocol used to move virtual computers from one physical host to another. Also used to move virtual machines from one data storage device to another.

IV. Resources / Contacts for IT Security

The contacts listed below may be considered as a consultant to assess the status of cybersecurity of the entity's network system, or assist with the implementation of these minimum standards, or provide emergency assistant in the event of a cybersecurity breach.

IT for Education

Julio Lopez
Office : 305.403.7582
jlopez@itforedu.com
www.itforedu.com

Visual Edge IT
Mark Jessup
Office: 954.860.0371
mjessup@visualedgeit.com
www.visualedgeit.com

ImageNet
Isaac Noguera
786.235.0222
jnoguera@imagenet.com
www.imagenet.com

VNET Consulting
Victor De La Torre
Office : 305.685.5555
vdelatorre@v-net.cc
www.v-net.cc

CyberSphere Solutions
Carlos Nunez
Office : 786.414.5595
cnunez@cyberspheresolutions.tech
cyberspheresolutions.tech

Assessing and advising regarding the status of the entity's cybersecurity:

Erik Brown, Business Information Security Officer for FACTS/Nelnet: EBrown@factsmgt.com. Nelnet manages federal student loan programs for universities, so they have expertise in cybersecurity (Nelnet owns FACTS). The blog provides references to webinars: From Threats to Tactics: Strengthening Cybersecurity in K-12 Education - FACTS Management.

Information Technology Assessment
Verdeja & Alvarez, LLP
Octavio A. Verdeja
Certified Public Accountants and Advisors
255 Alhambra Circle, Suite 630
Coral Gables, FL 33134
305.446.3177
oaverdeja@va-cpa.com

Initial: July, 2025
Current: