Archdiocese of Seattle

Mandatory Archdiocesan Digital Security Requirements
February 2026

SUMMARY

Given the exponential increases in cybersecurity incidents across the Archdiocese of Seattle, all Archdiocesan entities (parishes, schools, ministries, Chancery, etc.) will be required to adopt an enhanced security platform. There are two options:

- The Archdiocesan Guardian Platform is the recommended platform.
- Comparable security platform with vendor support is permitted if the vendor agrees to participate in the archdiocesan enhanced security initiative.

THE CHALLENGE

Today's Landscape: Cybercriminals are Targeting Parishes and Schools

Increasingly, across the archdiocese, parishes, schools and the Chancery are the targets of cybercriminals exploiting staff, systems and financial resources. What was a "once-in-a-while" event, is now frequent with sophisticated attacks from around the world. Entities within the archdiocese have recently experienced:

- **Credential Theft** – Cybercriminals stealing employee logins and using them to gain access to an employee Paycom account, rerouting paychecks away from the employee's bank account and into their personal bank account.

- **Document Sharing Exploits** – Cybercriminals capture a user's "Two-factor Authentication Token" and use it to share infected files with people listed in the email contact list.

- **Impersonated Archdiocese Communications** – Cybercriminals have impersonated email accounts, sending fake Chancery invoices and wire instructions to parishes and schools.

- **Parish Staff Impersonation** – Cybercriminals are also impersonating priests, deacons and parishioners to attempt to get parish staff to share sensitive information.

Today's cyber risks are more sophisticated, frequent, and damaging than ever before.

Ransomware continues to be a top threat, with attackers encrypting critical data and demanding payment for its release. Phishing and social engineering attacks are also widespread, often disguised as legitimate emails or messages that trick users into revealing passwords or sensitive information. AI is now used to develop more sophisticated targeted attacks and adaptive malware that evades traditional defenses.

Simultaneously, parish, school and ministry staff are not prepared to effectively combat today's evolving cybercrime landscape. Unfamiliar with the latest cyber threats, they are at a loss to identify, isolate, and remediate sophisticated hacking activities. As the threat landscape continues to evolve, so too must our ability to effectively combat these cybercriminals, with the adoption of a highly secure computing environment.

THE SOLUTION

Highly secured computing environment

Although Microsoft 365 (M365) offers a robust suite of built-in security features, it is not enough to ensure protection against today's evolving cyber threats. M365 primarily focuses on securing its own ecosystem—email, collaboration tools, and cloud storage—but lacks advanced threat detection, response capabilities and coverage for third-party apps or on-premises infrastructure. It also assumes that users configure security settings correctly, leaving gaps if policies are misconfigured or overlooked.

Although Gmail offers strong baseline security features such as spam filtering, two-factor authentication and AI-driven phishing detection, it is not sufficient as a standalone defense in today's complex threat landscape. Gmail lacks advanced threat intelligence, deep forensic capabilities, and broad visibility across an organization's full digital footprint. Additionally, relying solely on Google's security leaves organizations vulnerable to user misconfigurations, insider threats and sophisticated attacks that bypass basic filters. For true security, organizations need layered defenses, continuous monitoring, and integration with broader cybersecurity.

Given the increasing frequency and sophistication of cyber threats targeting religious institutions, **all Archdiocese of Seattle parishes, schools and ministries must adopt an enhanced security platform** to protect sensitive data, financial systems and the personal information of parishioners and staff.

This platform must include advanced threat detection, secure communication tools, multi-factor authentication and continuous monitoring to ensure the integrity and confidentiality of operations. The Church has a moral and legal obligation to safeguard its digital environment, just as it does its

physical spaces. By implementing a standardized, robust cybersecurity framework across all parishes, we uphold our commitment to stewardship, trust, and the responsible management of the Church's digital and human resources.

Packaged Offering – AOS Guardian Platform

The AOS Guardian Platform, a packaged offering available to archdiocesan parishes and schools, is designed to add enhanced security capabilities, adherence to archdiocesan policies and deliver capabilities well beyond what's currently in place at parishes and schools. Highly automated, administrative tasks such as centralized device management, backup and restore, virus and malware detection and archives continuously reduce the risk of nefarious actors infiltrating technology infrastructure. Professionally monitored and maintained, the Guardian Platform is a key component of the archdiocese's cyber defense infrastructure.

Benefits of the AOS Guardian Platform:

- ***Secure*** – Communications and computing within parish and/or school are secure and private. Threat remediation can quickly address potential exploits across the entire ecosystem.
- ***Professional support*** – Administrative functions are performed by industry professionals providing unparalleled support for parishes and schools.
- ***Features*** – In delivering capabilities beyond existing standards, the Guardian Platform adds additional endpoint protection against malware penetration and virus infection.
- ***Simple administration*** - Administrative responsibilities – such as adding users, backup and restore, archiving and others - are removed from your staff members.
- ***Two-factor authentication*** – This feature protects against stolen identities.
- ***Staff security awareness training*** – Industry Leading (KnowBe4) online security awareness training is part of the Guardian Platform. This training is key to keep everyone safe. The simple and short online modules make it easy to bring staff up to speed on how to spot security threats, phishing and more.

Alternative Platform Solutions

The AOS Guardian platform is preferred and recommended, but other enhanced protection environments may be acceptable. If a technology vendor can provide an enhanced protection environment that meets or exceeds the capabilities of AOS-Guardian, that solution is acceptable.

However, a critical condition of operating within such an environment is that the vendor must agree to participate in our enhanced security initiative. This means the vendor must promptly notify the archdiocese upon discovering any exploited system or compromised user. And each vendor will be notified when an exploit is identified. This early communication is essential to contain any breach and coordinate an effective, organized response. This collaborative approach also ensures a unified and proactive defense across all participating entities.

Her are the minimum requirements for an alternative security platform:

- ***Defense in Depth*** - Defense in Depth is a cybersecurity strategy that employs multiple layers of security controls to protect an organization's information and systems. Instead of relying on a single defense mechanism, it combines technologies, policies, and practices—such as firewalls, antivirus software, encryption, access controls, and employee training—to create a comprehensive shield against threats. If one layer is bypassed or fails, other layers will still provide protection, reducing the risk of a successful attack. This approach helps organizations address a wide range of vulnerabilities, making overall security more resilient and adaptive.

- ***System support and monitoring*** - Managed Detection and Response (MDR) is a proactive cybersecurity service that combines advanced technology with expert human analysis to continuously monitor, detect, and respond to cyber threats. Unlike traditional security tools that rely solely on automated alerts, MDR provides real-time threat hunting, incident investigation, and rapid response to contain and mitigate attacks. This service is especially valuable for organizations that lack the resources or expertise to maintain a full security operations center, as MDR providers deliver specialized skills and 24/7 monitoring. By quickly identifying and addressing sophisticated threats, MDR helps minimize damage, reduce downtime, and strengthen an organization's overall security posture.

- ***Endpoint protection*** - Endpoint protection refers to the security of individual devices—such as computers, smartphones, tablets, and servers. These devices, known as endpoints, are often entry points for cyberattacks within a network. Endpoint protection solutions typically include antivirus software, firewalls, intrusion detection systems, and more advanced technologies like behavioral analysis and threat intelligence. The goal is to monitor, detect, and respond to potential threats in real-time, ensuring that sensitive data remains protected, and that the overall integrity of the network is maintained.

- ***Device management (Windows)*** - Microsoft Intune is a cloud-based endpoint management solution that helps organizations manage and secure employee devices, whether they are

parish-owned or personal (BYOD). It enables IT administrators to control how devices are used and to enforce security policies across smartphones, tablets, and computers. Intune integrates with other Microsoft services like Azure Active Directory and Microsoft 365, allowing for streamlined user authentication, app deployment and data protection. With features like remote wipe, app management, and conditional access, Intune ensures sensitive corporate data remains secure while providing employees the flexibility to work from anywhere.

- ***Device management (MacOS)*** - JAMF is a comprehensive device management solution for Apple devices, including Macs, iPhones, iPads, and Apple TVs. It enables organizations to efficiently deploy, configure, manage and secure Apple hardware. With features like zero-touch deployment, app management, security compliance, and remote support, JAMF helps IT teams streamline operations while ensuring consistent user experience. Its strong integration with Apple's ecosystem allows for seamless updates and policy enforcement, making it a trusted tool for organizations that use Apple technology.

- ***Two-factor authentication*** - Two-Factor Authentication (2FA) is a security measure that adds an extra layer of protection to user accounts by requiring two forms of verification before granting access. Typically, this involves something the user knows—like a password—and something the user has—such as a mobile device, hardware token, or authentication app. Even if a password is compromised, 2FA significantly reduces the risk of unauthorized access because the attacker would still need the second factor. Widely used, 2FA is a simple yet effective way to strengthen account security and protect sensitive data from cyber threats.

- ***Security awareness training*** - Security awareness training is an educational program designed to inform and equip employees with the knowledge and skills needed to recognize and respond to cybersecurity threats. The training typically covers topics such as phishing attacks, password security, social engineering, safe internet practices, and data protection. Its primary goal is to reduce human error — the leading cause of security breaches — by promoting a culture of vigilance and responsibility. By regularly engaging employees with realistic scenarios and updated threat information, security awareness training helps organizations strengthen their overall security and minimize the risk of data loss or compromise.

- ***Cloud backup and restore*** - Cloud backup and restore is a data protection strategy that involves copying and storing files, applications, or entire systems in a secure, remote cloud environment. This ensures that data can be recovered in the event of accidental deletion, hardware failure, cyberattack or natural disaster. Cloud backup solutions typically offer

automated, scheduled backups and allow for scalable storage. The restore function enables users to quickly retrieve lost or corrupted data, often with options for restoring specific files or full system images. By leveraging the cloud, organizations benefit from off-site redundancy, enhanced security, and greater flexibility in disaster recovery planning.

Compatible Solutions

For a complete list of approved Guardian Platform Vendors, please visit the Archdiocese of Seattle Information Technology website: https://archseattle.org/InformationTech.

Adoption of the AOS Guardian Platform or Equivalent Security Solution

As part of the ongoing commitment to safeguarding the digital infrastructure of the archdiocese, all parishes, schools and ministries must implement the AOS Guardian Platform — or an equivalent, approved security and compliance solution.

This initiative is designed to strengthen our collective cybersecurity posture, ensure compliance with archdiocesan and regulatory standards, and provide centralized visibility into the health and security of our systems.

Adoption Timeline

- Start Date: February 1, 2026
- Parishes - Completion Deadline: December 30, 2026
- Schools - Completion Deadline: December 30, 2026

All institutions must complete their migration within this timeframe.

What You Need to Do

- **Engage an authorized vendor**
  Begin by contacting an authorized Guardian Platform vendor to initiate migration planning. These vendors are trained and approved to support deployment, configuration, and ongoing management of the platform. A list of approved vendors is available at: https://archseattle.org/InformationTech.

- **Assess current environment**
  Work with your vendor to evaluate your existing systems, identify any gaps, and determine hardware or software upgrades needed to support the platform.

- **Develop a migration plan**
  Establish a timeline for implementation that aligns with operational needs and the archdiocesan deadline. Include staff training, testing, and contingency planning.

- **Implement and validate**
  Complete the deployment of the Guardian Platform or equivalent solution, ensuring all required security policies, monitoring tools, and compliance checks are in place.

Why This Matters
The AOS Guardian platform provides:

- Real-time visibility into system health and compliance
- Automated enforcement of security policies
- Protection against misconfigurations and vulnerabilities
- Centralized reporting and audit readiness

Failure to adopt a compliant solution may result in increased risk exposure and non-compliance with Archdiocesan IT standards.

Appendix – Independent Adoption and Guardian Platform Training

Individuals or departments that choose to adopt and implement AOS Guardian Platform capabilities tools independently—outside of a centrally coordinated rollout—assume responsibility for ensuring compliance with all training, usage and operational requirements of the Guardian Platform.

ADMINISTRATION

Organizations that elect to adopt the AOS Guardian requirements independently assume complete responsibility for the administration of their local platform(s). This includes all tasks related to configuration, user management, security settings, and ongoing maintenance. Additionally, these parishes are accountable for monitoring system health, applying updates, and ensuring compliance with all relevant policies and standards. By choosing independent adoption, the parish becomes the sole administrator and must manage every aspect of the platform without reliance on centralized support.

Organizations that outsource compliance activities to unapproved third-party providers also inherit full responsibility for meeting AOS Guardian compliance requirements. Engaging such providers does not transfer accountability; the parish remains liable for ensuring that all standards, controls, and reporting obligations are properly implemented and maintained.

Core Administrative Policies

1. **Conditional Access Policies**
   - Require compliant devices for access to M365 resources
   - Enforce device-based Conditional Access that binds tokens to specific devices
   - Implement Continuous Access Evaluation (CAE) to enable near real-time token revocation
   - Block legacy authentication protocols completely
   - Require multi-factor authentication for all users, especially administrators

2. **Token Lifetime Management**
   - Configure shorter token lifetimes (default is 1 hour for access tokens)
   - Reduce refresh token maximum age from the default 90 days to 14-30 days for sensitive accounts
   - Enable "Remember MFA" with shorter durations (no more than 7 days)

- Consider disabling persistent refresh tokens entirely for high-risk roles

3. **Device Management**
   - Require device enrollment in Intune or Endpoint Manager
   - Enforce device compliance policies before allowing access
   - Enable Token Protection (a Windows security feature that binds tokens to hardware)
   - Block access from unmanaged devices for sensitive workloads
   - Regularly audit device compliance status

4. **Session Management**
   - Configure sign-in frequency policies to require re-authentication every 1-8 hours for sensitive apps
   - Enable persistent browser sessions only on managed devices
   - Implement Azure AD Smart Lockout to prevent brute force attacks

5. **Identity Protection**
   - Enable Azure AD Identity Protection to detect risky sign-ins and compromised credentials
   - Configure risk-based Conditional Access policies that require password reset or MFA step-up for risky sessions
   - Automate token revocation when risk is detected
   - Enable sign-in risk and user risk policies with appropriate remediation actions

6. **Administrative Account Protection**
   - Enforce phishing-resistant MFA (FIDO2, Windows Hello for Business, or certificate-based authentication) for privileged accounts
   - Implement Privileged Access Workstations (PAWs) for admin tasks
   - Use Azure AD Privileged Identity Management (PIM) with just-in-time access
   - Require fresh authentication for admin actions (set sign-in frequency to 1 hour or less)
   - Prohibit persistent tokens for privileged roles

7. **Email Delivery Filter Protection Policy**
   Policy Objective: Restrict the ability to create, modify, or delete email delivery filters (inbox rules, transport rules, and mail flow rules) to designated trusted administrators only.
   - Exchange Online Inbox Rules Protection
   - Disable End-User Inbox Rule Creation:

Remove the "MyMailboxDelegation" and "MyBaseOptions" RBAC roles from default users. Implement the following PowerShell policy:

 # Disable ability for users to create inbox rules via Outlook and OWA

Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AllowedInboxRules ClientOnlyRules

 # Or completely disable inbox rule creation

Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AllowedInboxRules None

8. **Application Security**
   - Audit and restrict application permissions through consent policies
   - Block applications that request offline access without business justification
   - Implement app protection policies to prevent data exfiltration
   - Use Microsoft Defender for Cloud Apps to monitor OAuth app activities

9. **Monitoring and Response**
   - Enable Azure AD audit logs and sign-in logs
   - Configure alerts for suspicious token activity (e.g., token replay, impossible travel)
   - Monitor for Primary Refresh Token (PRT) abuse
   - Implement SIEM integration for centralized monitoring
   - Create playbooks for token compromise incidents

10. **Network Controls**
    - Implement named locations in Conditional Access
    - Block or require MFA from unfamiliar locations
    - Use geo-blocking where appropriate for your organization
    - Consider requiring VPN or private network access for sensitive operations

TRAINING

Meeting AOS Guardian compliance standards is not limited to technology—it requires well-informed personnel who understand their roles and responsibilities. Proper training is essential to ensure that administrators, staff, and volunteers can effectively implement security controls, maintain compliance, and respond to emerging threats. All organizations adopting AOS Guardian, whether independently or through centralized support, are required to meet established training standards. These standards help safeguard sensitive data, reduce risk, and promote a culture of accountability across every parish.

- Microsoft 365 Certified: Fundamentals (MS-900)
- Microsoft 365 Certified: Security Administrator Associate (MS-102)
- Microsoft Certified: Endpoint Administrator Associate (MD-102)

OPERATIONAL RESPONSIBILITIES

Operational responsibilities are a critical component of AOS Guardian compliance. Every parish adopting the platform—whether independently or through centralized support—must ensure that day-to-day activities align with established security and governance standards. These responsibilities include maintaining system integrity, applying updates, monitoring for vulnerabilities, and enforcing access controls. Consistent execution of these tasks is essential to protect sensitive information, sustain compliance, and minimize risk. Meeting operational standards is not optional; it is a requirement that underpins the overall security posture of the organization.

On Demand

- For each incident observed – Message incident@seattlearch.org within 2 hours
- Upon remediation of the impacted client. Message incident@seattlearch.org
- For each incident alert from the archdiocese: Take the appropriate action as detailed in the alert (quarantine inbound messages from identified impacted user for example, remove quarantine, etc.).

Daily:

- Check security alerts and incidents
- Review Threat Explorer for new threats
- Monitor service health

Weekly:

- Review detection reports and trends
- Update allow/block lists as needed
- Check for policy violations

Monthly:

- Review Secure Score improvements
- Analyze phishing simulation results
- Update DLP policies based on incidents
- Review and adjust retention policies

Quarterly:

- Full security assessment
- Update protected users/domains
- Review and update incident response plan
- Conduct tabletop exercises

Annually:

- Comprehensive security audit
- Review all policies and update
- Assess new Microsoft 365 features
- Update training materials

Note:
The requirements outlined above are specifically applicable to implementations where Azure Entra ID serves as the primary source for identity and access management. In scenarios where a Parish opts to use a locally managed identity provider (IDP)—such as Microsoft Active Directory—for a single-purpose deployment, it is essential that the same level of security controls and standards are upheld. This includes, but is not limited to, authentication protocols, access policies, audit logging, and identity lifecycle management. The goal is to ensure equivalent security posture regardless of the IDP platform in use, thereby maintaining consistency across environments and safeguarding sensitive systems and data.