AOS-365 Platform – Archdiocese of Seattle

The AOS-365 Platform, an optimized version of Microsoft's 365 infrastructure, designed to add enhanced security capabilities, adherence to Archdiocesan policies and deliver capabilities well beyond Microsoft's M365 standard platform. Highly automated, administrative tasks such as centralized device management, backup & restore, archives and virus & malware detection continuously reduces the risk of nefarious actors penetrating your infrastructure. Professionally monitored and maintained, the ARCH365 tenant is a key component of the archdiocese's cyber defense infrastructure.

Overall Benefits of a Unified Master Microsoft 365 System

Secure – Communications and Compute within your 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 your Parish and/or School.

Features - Capabilities beyond the standard Microsoft M365 platform.

Administrative Responsibilities, adding users, backup & restore, archiving and others are removed from your staff members.

Two-Factor Authentication – To protect against stolen identities.

Security Awareness Training – Industry Leading (KnowBe4) security awareness training for your staffs.

Important Considerations

To provide the highest possible security, some advanced administrative Microsoft 365 features are not available to users of AOS-365. To preserve privacy between Parishes and Schools, the ability to manage users and their access to services is reserved to the administrators of the platform. This restriction exists to overcome the fact that Microsoft only supports administrative capabilities globally across the AOS-365 Platform. This restriction also impacts the ability to add capabilities from some 3rd-party tools to preserve the security boundaries.

Likewise, to protect from the leakage of personally identifiable information, the ability to redirect email outside of the boundaries system his highly regulated, and in most cases not available to preserve the backup, security and archival capabilities of the platform.

As a key component to ensure the privacy of the platform, the Platform acts as a "Walled Garden", one where Chancery IT has no access to the communication traversing it.

Adoption

An Archdiocese-wide adoption requirement goes into effect July 1, 2025, planned to be fully completed by June 30, 2026.

Detailed Capabilities of a Unified Master AOS-365 System

1. Security and Compliance
   - Industry-Standard Security: Built to meet rigorous security specifications, safeguarding user data and business information.
   - Reduced Attack Surface: Centralized tenant minimizes vulnerabilities.
   - Secure Communications: Ensures private and secure communication within and between organizations, including the Chancery.
   - Rapid Threat Response: Centralized management enables quick mitigation of emerging threats.
   - Clear Data Segmentation: Protects individuals by separating personal and corporate data.
   - Enhanced Data Protection: Comprehensive security stack includes file protection services and redundant backups.
   - Shared Security Insights: Data from one organization enhances protection for all.
   - Two-Factor (2FA) Authentication.
   - Security Awareness Training for staff members.
2. Economies of Scale
   - Cost Savings: Centralized pricing benefits are distributed across the entire organization.
   - Global Updates: Policy and security changes can be implemented across all sub-organizations, reducing individual IT costs.
3. Unified Resources
   - Streamlined Communication: Improved collaboration across parishes and between sub-organizations through:
     - Email
     - Microsoft Teams

- Teams Calling
- File sharing
- Contact sharing
- Simplified Account Management: Facilitates easier account and data transfers within parish families.
- Resource Optimization: Enables pooling of IT and communication resources within parish families, improving efficiency and supporting better budget management.

4. Improved Collaboration and Productivity
- Seamless Integration: Unified tools (e.g., Microsoft Teams, SharePoint, OneDrive) enhance collaboration across the organization.
- Consistent User Experience: Standardized systems provide a familiar interface for users, reducing learning curves and improving efficiency.
- Real-Time Collaboration: Supports simultaneous editing and sharing of documents across teams and locations.
- Cross-Parish Collaboration: Supports Teams features between users of the ARCH365 Platform. Easily share files and calendars between Parish Family Members.

5. Centralized IT Management
- Simplified Administration: Centralized control over user accounts, permissions, and policies reduces IT workload and ensures consistency.
- Automated Processes: Tools like Power Automate and compliance workflows streamline routine tasks across the organization.
- Scalability: Easily onboard new users or sub-organizations without creating duplicate or redundant resources.

6. Business Continuity
- Disaster Recovery: Built-in redundancy and backups ensure data integrity and availability in case of incidents.
- Reduced Downtime: Centralized troubleshooting and support minimize disruptions.

7. Compliance with AOS Cyber-Insurance guidelines
- The switch to AOS-365 reinforces our commitment to our insurance carrier partners, that we are adjusting our cyber security policies to meet present day challenges and demands.
- This approach not only protects CCAS and its data, ARCH365 may support a reduction in cyber security insurance costs paid for by member parishes & schools.

- In enforcing the necessary tools to protect our software & data, AOS-365 avoids the potential violation of the insuring agreement we have with our cyber insurance carrier, in the event a breach occurs.
- AOS-365 avoids unnecessary risk exposure, created where access to CCAS data (at all levels throughout the organization) is compromised and accessed by bad actors.

8. Compliance with Legal and Regulatory Standards
   - Standardized Policies: Ensures all sub-organizations can easily adhere to consistent policies for compliance with regulatory standards as needed (GDPR, HIPAA, PCI, etc.).
   - Audit Readiness: Centralized logs and compliance tools simplify audit preparation and reporting

9. Long-Term Sustainability
   - Future-Ready: Centralized systems make it easier to adopt new technologies or respond to industry changes.

10. Enhanced Support for Smaller Organizations
    - Access to Enterprise-Grade Tools: Smaller parishes benefit from high-quality tools and services that may have been cost-prohibitive independently.
    - Shared Expertise: Access to centralized IT expertise provides support and guidance that smaller entities might lack.

11. Built to adhere to Archdiocesan Policies
    - Electronic Communications: https://archseattle.org/wp-content/uploads/2021/02/ElectronicCommunications.pdf
    - Technology Access Policy: https://archseattle.org/wp-content/uploads/2024/07/202405CCAS-Technology-Access-Policy-min.pdf
    - Technology Acceptable Use Policy: https://archseattle.org/wp-content/uploads/2024/07/202405CCAS-Technology-Acceptable-Use-Policy-min.pdf
    - Security System Management Policy: https://archseattle.org/wp-content/uploads/2024/07/202401CCAS-Security-System-Management-Policy-min.pdf
    - Information Security Program: https://archseattle.org/wp-content/uploads/2024/12/CCAS-Information-Security-Program-Final-2024-January-min.pdf
    - Archives and Record Management Policies: https://archseattle.org/about-the-archdiocese-of-seattle/archives-and-records-management-public/archives-and-records-management_policies_resources/