RCAA
ADMINISTRATIVE SERVICES, INC.

Memo

Date: November 3, 2025

To: Pastors, principals and parish and school business managers

From: Holly Orsagh, director of financial services, Office of Finance

Re: Multi-factor authentication (MFA) policy

Due to an increase in compromised emails at archdiocese parishes and schools, we recommend that all parishes and schools adopt the following or a similar multi-factor authentication (MFA) policy. Not having MFA on Microsoft 365 environment increases the risks of data takeover, malware distribution, phishing from compromised accounts, unauthorized access to other connected services, major operational disruptions and financial losses. It may also lead to increased cyber security premiums.

For questions regarding the status or MFA or implementing it in your Microsoft 365 environment, contact your IT service provider. For advice on this topic, contact Tom Hardy, archdiocesan director of Information Technology, at thardy@archatl.com or 404-920-7454.

Purpose

The purpose of this policy is to protect (enter name of church and school)'s Microsoft 365 environment, member data, financial systems and other sensitive information from unauthorized access by mandating the use of multi-factor authentication (MFA) for all user accounts.

Scope

This policy applies to all individuals who access (enter name of church and school)'s Microsoft 365 accounts, including staff, pastors, volunteers, board members and contracted IT personnel. It covers all (ennter name of church and school)-owned or affiliated Microsoft 365 accounts, regardless of access level.

Policy Statement

RCAA
ADMINISTRATIVE SERVICES, INC.

All Microsoft 365 accounts under (enter name of church and school)'s domain must be secured with multi-factor authentication. No user shall have access to Microsoft 365 services—including but not limited to Outlook, OneDrive, Teams, SharePoint and the Microsoft 365 admin center—without completing MFA registration and use. An every (enter # of days – we recommend 7) day authentication is used.

Definitions

- **Multi-Factor Authentication (MFA):** A security process requiring two or more separate methods for verifying a user's identity before granting system access.
- **Microsoft Authenticator App:** The church and school's preferred method for MFA verification. Use of SMS or email-based MFA is allowed only as a backup.

Requirements

1. **Mandatory Enrollment:**
   All users must register for MFA using the microsoft authenticator app as part of account onboarding. Existing users must enable MFA within 30 days of this policy's issuance.

2. **Approved Authentication Methods:**
   - App-based authentication via Microsoft authenticator (preferred)
   - Hardware token (for users unable to use the app)
   - SMS code (temporary or fallback only)

3. **Access Enforcement:**
   Conditional access policies will enforce MFA for all users through Microsoft Entra ID. Legacy sign-in methods without MFA (such as basic authentication) will be blocked.

4. **Administrative Access:**
   All administrative accounts must use MFA at every sign-in attempt without exception.

5. **High-Risk Sign-ins:**
   Users identified as signing in from new countries, devices or suspicious networks will be required to reauthenticate using MFA before access is granted.

6. **Service Accounts:**
   Interactive logins for service/system accounts are prohibited. Service accounts must be migrated to secure workload identities.

7. **Ongoing Compliance:**
   The IT administrator will perform quarterly audits to verify MFA compliance and generate reports for leadership review.

Exceptions

Temporary exceptions (e.g., technical inability to authenticate) must be pre-approved in writing by the pastor or principal after review of the church's IT administrator and remediated as soon as practical. No permanent exceptions are permitted.

Responsibilities

- **IT Administrator:** Enforces MFA through Microsoft Entra Conditional Access, monitors compliance and assists users with setup.
- **All Users:** Must maintain MFA-enabled devices securely and report lost or compromised devices immediately.

Enforcement

Failure to comply with this policy will result in account suspension until MFA is enabled. Repeated violations may result in loss of Microsoft 365 access privileges.

Review and Revision

This policy shall be reviewed annually or as needed to comply with changes in Microsoft security requirements or evolving cybersecurity threats.

This model aligns with Microsoft's 2025 mandatory MFA enforcement in Microsoft 365 and Azure environments and is written to be inserted directly into a church's IT or data security policy manual.