SMB Security Enhancement Strategy

# 1. Purpose & Scope

This document outlines a proposed security enhancement strategy for a small-to-medium business (SMB) undergoing modernization. The goal is to strengthen the security posture across endpoints, identities, and data using best practices aligned with modern tools such as Microsoft Defender, Azure AD, and Intune.

# 2. Identity and Access Management (IAM)

- Implement Azure Active Directory with hybrid sync (via Azure AD Connect)  
- Enforce Multi-Factor Authentication (MFA) for all users  
- Apply conditional access policies (e.g., block legacy auth, restrict by location)  
- Conduct regular access reviews and permission audits

# 3. Endpoint Protection and Compliance

- Enroll all corporate devices into Microsoft Intune  
- Apply Microsoft security baselines (e.g., password policies, encryption)  
- Enable Microsoft Defender for Endpoint (EDR, antivirus, threat protection)  
- Set up compliance policies to prevent non-compliant device access

# 4. Data Protection and Backup

- Implement Microsoft 365 data retention and DLP policies  
- Use OneDrive and SharePoint for secure cloud storage with version history  
- Configure Azure Backup or third-party backup solutions for critical data  
- Enable mailbox auditing and alert policies for sensitive activities

# 5. User Awareness and Training

- Conduct regular phishing simulations and security awareness campaigns  
- Provide training on MFA, secure password practices, and data handling  
- Maintain an internal security knowledge base or FAQ site

# 6. Monitoring and Incident Response

- Use Microsoft Defender dashboards to monitor threat activity  
- Set up alerting for high-risk sign-ins and unusual behaviors  
- Develop and document an incident response plan for handling breaches  
- Conduct tabletop exercises and post-incident reviews

# 7. Continuous Improvement

- Schedule quarterly reviews of security configurations  
- Subscribe to CVE feeds and Microsoft Security advisories  
- Regularly assess logs, security score, and threat reports to identify gaps