NEXTGRID TECHNOLOGIES

M365 SECURITY CHECKLIST 2026

12 Steps to POPIA Compliance & Ransomware Protection

Microsoft 365 is the #1 target for SA cyber-attacks. Use this checklist to audit your tenant in 15 minutes.

Fail 3+ items? You're at high risk. POPIA fines reach R10M.

■ 1. MFA ENFORCED FOR ALL USERS

Microsoft Authenticator app only. SMS disabled. No exceptions.
POPIA: You must protect account access.

■ 2. LEGACY AUTHENTICATION BLOCKED

Old mail apps bypass MFA. Disable in Azure AD > Security.
PowerShell: Get-AzureADPolicy | ? {$_.Type -eq "BlockLegacyAuth"}

■ 3. SEPARATE ADMIN ACCOUNTS CREATED

Never use daily email as Global Admin. Create admin@company.onmicrosoft.com

■ 4. CONDITIONAL ACCESS: BLOCK FOREIGN LOGINS

Block Nigeria, Russia, China if you don't operate there. Require compliant devices.

■ 5. MAILBOX AUDITING ENABLED

Turned OFF by default. Required for POPIA breach investigations.
PowerShell: Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true

■ 6. SAFE LINKS & SAFE ATTACHMENTS ON

Stops 99% of phishing. Requires Defender for Office 365 P1 or Business Premium.

■ 7. AUTO-FORWARDING TO EXTERNAL BLOCKED

Common attacker tactic. Block in Exchange Admin > Mail flow.
PowerShell: Get-RemoteDomain | Set-RemoteDomain -AutoForwardEnabled $false

■ 8. DATA LOSS PREVENTION (DLP) CONFIGURED

Auto-block ID numbers, bank details from external email. POPIA requirement.

■ 9. OAUTH APP PERMISSIONS REVIEWED

Revoke "Mail.ReadWrite" from dodgy apps. Attackers buy tokens on dark web.
Check: Azure AD > Enterprise Applications > Permissions

■ 10. UNIFIED AUDIT LOG: 1 YEAR RETENTION

Default is 90 days. POPIA requires 1 year. Change in Purview > Audit.

■ 11. ALERTS: NEW GLOBAL ADMIN + PRIVILEGE ESCALATION

Get SMS if someone makes themselves admin. Security & Compliance > Alerts

■ 12. IMMUTABLE CLOUD BACKUPS ACTIVE

M365 recycle bin ≠ backup. Ransomware deletes it. Use Veeam/Acronis/Afrihost.
Must backup: Exchange, OneDrive, SharePoint, Teams.

SCORE YOUR RISK:

0-2 Failed = Low Risk. Good job. Review quarterly.
3-5 Failed = Medium Risk. Fix within 7 days.
6+ Failed = HIGH RISK. You're 1 click from a breach. Act today.

FAILED 3 OR MORE ITEMS?

You're at high risk. We do a 3-Day M365 Hardening Sprint for Gauteng businesses. Zero downtime.

Book your R950 IT Health Check:
https://www.nextgridtechnologies.co.za/r950-check.html
Or WhatsApp: 068 033 0794