M365 Security Checklist 2026

NextGrid Technologies • Microsoft 365 Authorized • Lenovo 360 Authorized 2026 • POPIA Ready

For SA SMEs 5-50 staff • Pretoria on-site, remote SA • Secure Score 42% → 85% in 3 hours • Avg 4.2 critical issues found in R950 Check • Call +27 76 948 9154 • info@nextgridtechnologies.co.za

How to use: Tick each item. If you cannot tick it, you are exposed. This is the exact checklist we use for our R2,290 M365 hardening (same-day, no downtime). Based on 47 SME audits 2025-2026. Maps to POPIA 8 conditions.

1. IDENTITY & MFA – Stop 99% of logins (POPIA Condition 7: Security Safeguards)

- ■ MFA enforced for ALL users (not just admins) – number matching enabled, no SMS codes
- ■ Legacy authentication blocked (Basic Auth, POP, IMAP, SMTP Auth disabled via Conditional Access)
- ■ MFA fatigue / number matching – user must enter number shown on screen
- ■ Break-glass admin accounts secured – 2 emergency accounts, FIDO2 key, excluded from CA, monitored
- ■ Self-service password reset (SSPR) enabled with MFA, no helpdesk password resets via phone
- ■ Passwordless option for directors – Windows Hello for Business / FIDO2
- ■ User risk policy – medium/high risk forces password reset + MFA
- ■ Admin accounts are separate – no day-to-day email on Global Admin, Privileged Identity Management (PIM) for 5-50 staff

2. CONDITIONAL ACCESS – Block logins outside SA

- ■ Conditional Access: Block logins outside South Africa + trusted locations only
- ■ Block impossible travel (login SA then US in 10 min = blocked)
- ■ Require compliant device OR hybrid joined for M365 apps – block personal unmanaged devices for finance
- ■ Sign-in frequency – 8 hours for finance, 24 hours for others
- ■ Block risky sign-ins – anonymous IPs, TOR, malware-linked IPs blocked via Entra ID Protection
- ■ Legacy protocols audit – report shows 0 legacy auth in last 30 days

3. EMAIL SECURITY – Safe Links & Safe Attachments (Stops BEC even if user clicks)

- ■ Safe Links enabled – every URL rewritten and checked at click time (including Teams, Office docs)
- ■ Safe Attachments enabled – attachments detonate in sandbox before delivery, 5 min delay acceptable for SMEs
- ■ Anti-phishing policy – impersonation protection for CEO, finance, director display names + domains
- ■ External email banner – [EXTERNAL] banner + first-contact safety tip for all external senders
- ■ Mailbox forwarding / auto-forward to external blocked (common BEC persistence)
- ■ Inbox rules audit – check for attacker-created rules forwarding to Gmail/evil domain (found in 18% of audits)
- ■ Mailbox auditing enabled – 1 year audit log retention for POPIA evidence
- ■ Disable auto-forward to external via outbound spam filter + transport rule

4. DMARC / SPF / DKIM / ANTI-SPOOF – Block lookalike domain invoice scam (R87k case)

■ SPF record: v=spf1 include:spf.protection.outlook.com -all (hard fail, not ~all)

■ DKIM enabled and rotated for all custom domains in Exchange Online

■ DMARC record: v=DMARC1; p=quarantine; rua=mailto:dmarc@nextgridtechnologies.co.za; pct=100; fo=1 (then p=reject after 2 weeks)

■ Anti-spoof intelligence + spoof intelligence insight enabled, quarantine spoofed emails

■ Domain-based impersonation protection – protect nextgridtechnologies.co.za + client domains + CEO names

5. DEVICE SECURITY – Intune, BitLocker, Defender for Endpoint

■ Intune enrollment – all Windows devices auto-enroll, compliance policy: BitLocker + Defender + min OS version

■ BitLocker enforced – recovery keys escrowed to Entra ID, 0 devices unencrypted (check in Intune)

■ Microsoft Defender for Business – all devices onboarded, tamper protection on, attack surface reduction rules

■ Local admin disabled via LAPS – no user is local admin day-to-day (blocks ransomware lateral movement)

■ Windows Hello for Business or FIDO2 – PIN/biometric, no password spray possible

■ Compliance → Conditional Access – non-compliant device = block M365 access

6. DATA PROTECTION – DLP, Encryption, Retention (POPIA Conditions 6 & 7)

■ DLP policy – block SA ID numbers, bank account numbers, passport numbers from leaving via email/Teams/SharePoint

■ Email encryption – OME enabled, finance must encrypt invoices with ID numbers / sensitive docs

■ Retention labels – 7yr invoices (Tax Admin Act), 1yr CVs auto-delete (POPIA), 3yr Teams chats – auto-applied in Purview

■ Sensitivity labels – Confidential / Internal / Public, auto-label for ID numbers

■ Customer Lockbox + Purview audit – no Microsoft access without approval, 1yr audit log

■ OneDrive known folder move + backup – Desktop/Documents/Pictures backup + 90-day versioning + immutable backup separate from OneDrive (OneDrive is NOT backup)

■ SharePoint sharing – external sharing = only people with link + expiration 30 days + no anonymous links for finance

7. ADMIN & MONITORING – 24/7, Secure Score, POPIA Evidence

■ Secure Score – baseline measured, target 85%+, monthly report to directors (we include in R950 report)

■ Alert policies – impossible travel, mass file deletion, inbox rule creation, eDiscovery search, admin consent – alert to info@ + WhatsApp

■ Audit log search enabled – Unified audit log on, 1 year retention for POPIA Condition 8: Accountability

■ Monthly access review – guest users, inactive users >90 days disabled, admin roles reviewed

■ Backup verification – M365 backup restore test monthly (real restore of mailbox + SharePoint, not just green tick) – immutable backup

POPIA 8 Conditions Mapping (for your auditor)

POPIA Condition	M365 Control in this checklist
1 Accountability	Audit log, access reviews, Secure Score monthly report

2 Processing Limitation	DLP blocks ID numbers leaving, retention labels auto-delete
3 Purpose Specification	Sensitivity labels, DLP purpose justification
4 Further Processing	DLP + retention prevents repurposing CVs beyond hiring
5 Information Quality	Intune compliance, Defender ensures clean data
6 Openness	External banner, sensitivity labels inform users
7 Security Safeguards	MFA, CA, Safe Links, BitLocker, Defender, encryption
8 Data Subject Participation	eDiscovery + retention allows subject access requests in 8 hours

What to do next – 3 steps, 3 days (NextGrid)

1. **Book R950 Health Check** – 2hr on-site Pretoria/Centurion/Midrand/JHB or remote SA. We run this checklist, test backup restore for real, check POPIA 8 conditions. Same-day 12-page PDF + Loom video. Pay after visit. 47 checked avg 4.2 critical.

2. **Fix & Secure (R2,290 one-time)** – We apply all controls in this checklist same week, no downtime. Secure Score 42% → 85%. 60-user manufacturer done in 3 days. Includes DMARC, Safe Links, Conditional Access SA only.

3. **Ongoing – M365 R290 + 24/7 monitoring** – One invoice for M365 Standard R290, Lenovo 360 hardware, POPIA-ready security. Unlimited helpdesk avg <1hr, monthly health report. No lock-in. Call +27 76 948 9154.