

Microsoft 365 security checklist.

The hardening controls our senior team applies on real Microsoft 365 tenants. Work top to bottom, identity first, it is where most breaches start.

01 Identity & access

- MFA for all users.** Enforced via Conditional Access, not per-user legacy settings
- Block legacy authentication.** POP/IMAP/SMTP basic auth disabled, it bypasses MFA
- Privileged Identity Management.** Just-in-time, time-boxed admin roles; break-glass account excluded and monitored
- Conditional Access.** Risk-based policies; block or step-up on risky sign-ins and unmanaged devices

02 Email & collaboration

- SPF, DKIM & DMARC.** All three published and DMARC moving to p=reject
- Safe Links & Safe Attachments.** Defender for Office 365 policies enabled
- Anti-phishing.** Impersonation and spoof protection on key users and domains
- External sender tagging.** Recipients see a clear external warning

03 Data protection

- Sensitivity labels.** Applied to classify and protect documents and email
- DLP policies.** Prevent accidental sharing of financial, health or PII data
- Sharing controls.** SharePoint/OneDrive external sharing scoped to business need

04 Devices

- Intune compliance.** Only compliant, encrypted, up-to-date devices reach company data
- Disk encryption.** BitLocker / FileVault enforced and keys escrowed

05 Monitoring & recovery

- Unified audit log.** Enabled and retained; alerts on risky admin actions
- Secure Score.** Reviewed regularly with a plan to improve it

Backup. Third-party backup of Exchange, SharePoint, OneDrive and Teams, native retention is not a backup

One quiet gap to check first: legacy authentication. It silently bypasses MFA and is behind a large share of M365 account takeovers, confirm it is blocked tenant-wide.

Want this assessed for your environment?

Book a 90-minute discovery & security session.

09 974 2379 · +61 3 4803 4915

belton.co.nz/get-started

This resource is a general, plain-English guide offered as-is and is not a substitute for tailored professional, legal or insurance advice. Frameworks referenced (ASD Essential Eight, Microsoft 365 security baselines, common cyber-insurance underwriting controls) are owned by their respective publishers. Belton IT Nexus Limited, NZ-owned since 2004.