Tenant Security
By CyPro

THE WORKING CHECKLIST

Microsoft 365 Security Checklist

The ten best practices that stop real attacks, in priority order. Mapped to the CIS Microsoft 365 Foundations Benchmark. From Tenant Security, a specialist service from CyPro Ltd.

Work top to bottom: the ordering reflects which misconfigurations feature most in real UK tenant compromises. Each item has a verification step so "done" means checked, not assumed.

1 Enforce MFA for every user through Conditional Access

Why it matters: Stolen passwords are the entry point for most tenant compromises; enforced MFA defeats the plain credential attack outright.

How to verify: Entra admin centre > Conditional Access: a policy requiring MFA for all users, all apps, with only a break-glass exclusion. Registration alone is not enforcement.

Owner: ..... Date checked: ..... Status: .....

2 Block legacy authentication protocols

Why it matters: IMAP, POP and SMTP basic auth ignore MFA entirely, which is why password-spray attacks target them first.

How to verify: A Conditional Access policy blocking legacy authentication clients, and sign-in logs filtered to legacy protocols showing no successful entries.

Owner: ..... Date checked: ..... Status: .....

3 Cut Global Administrator accounts to five or fewer

Why it matters: Every additional global admin is another account whose compromise means total tenant loss. CIS recommends two to four plus emergency access.

How to verify: Entra roles: count Global Administrator assignments; each must be a named person with a reason, plus one documented break-glass account.

Owner: ..... Date checked: ..... Status: .....

☐ **4** **Turn on unified audit logging and mailbox auditing**

Why it matters: Without the logs there is no investigation, only guesswork. This is the finding that turns incidents into unanswerable questions.

How to verify: Purview compliance portal > Audit: search enabled and returning events; Get-Mailbox reporting AuditEnabled true for all user mailboxes.

Owner: ..... Date checked: ..... Status: .....

☐ **5** **Disable or govern automatic email forwarding**

Why it matters: Silent forwarding rules to external addresses are the classic persistence trick in business email compromise cases.

How to verify: Exchange admin centre: outbound spam policy blocks auto-forwarding, and a transport rule report shows no unexplained external forwards.

Owner: ..... Date checked: ..... Status: .....

☐ **6** **Require admin consent for new app registrations**

Why it matters: OAuth consent phishing grants an attacker durable, MFA-proof access through an app your user approved in one click.

How to verify: Entra > Enterprise applications > Consent settings: user consent disabled or restricted to verified publishers with the admin consent workflow on.

Owner: ..... Date checked: ..... Status: .....

☐ **7** **Restrict anonymous and company-wide sharing links**

Why it matters: Anyone-links turn a single misjudged share into public exposure of client data; defaults matter more than policy documents.

How to verify: SharePoint admin centre: external sharing at the most restrictive workable level, default link type set to specific people.

Owner: ..... Date checked: ..... Status: .....

☐ **8** **Govern guest access with expiry and reviews**

Why it matters: Guests accumulate: every finished project leaves accounts with live access to your Teams and files.

How to verify: Entra > External identities: guest invite settings restricted, access reviews scheduled, and last quarter's review actually completed.

Owner: ..... Date checked: ..... Status: .....

☐ **9** **Deploy the anti-phishing stack you already own**

Why it matters: Safe Links, Safe Attachments and impersonation protection ship with Business Premium and above; unconfigured, they protect nobody.

How to verify: Defender portal > Email & collaboration policies: preset security policies applied, or custom policies covering all recipients.

Owner: ..... Date checked: ..... Status: .....

☐ **10** **Set retention before you need it**

Why it matters: Deleted evidence and unrecoverable mailboxes both trace back to retention decisions nobody made.

How to verify: Purview > Data lifecycle management: retention policies covering Exchange, SharePoint and OneDrive with periods your legal team recognises.

Owner: ..... Date checked: ..... Status: .....

Worked through the ten?

These checks close the doors attackers use most. The expert assessment reviews several hundred further settings in the context of your business, benchmarked against comparable UK tenants, with pricing published in full so you already know what it costs.

tenantsecurity.co.uk/pricing/