IT CLUB · CYBER SECURITY

HOW SECURE IS YOUR MICROSOFT 365 TENANT?

Microsoft 365 Security Baseline Checklist · IT Club · itclub.work

Seven controls every business should review

WARNING: Buying the security licence is not the same as implementing the security control.

1. **AUTHENTICATE** — MFA + Passkeys
2. **LIMIT** — Administrator access
3. **CONTROL** — External sharing
4. **TRUST** — Managed devices
5. **RECORD** — Audit activity
6. **STANDARDISE** — Security baseline
7. **REVIEW** — Risk + Secure Score

MICROSOFT 365 SECURITY = CONFIGURATION + REVIEW

CIS M365 FOUNDATIONS BENCHMARK

- Community-developed security benchmark
- Current version: v7.0.0 (June 2026)
- Level 1 — minimal operational impact
- Level 2 — higher-security environments
- Not a legal requirement or certification
- Verify current version at cisecurity.org

MICROSOFT SECURE SCORE

- Microsoft posture measurement tool
- Available: security.microsoft.com/securescore
- Covers Identity, Devices, Apps, Data
- Use to prioritise — not chase 100%
- Neither CIS nor Score = breach-proof
- Document: Implement / Accept / N/A / Defer

IT CLUB SECURITY MATURITY MODEL (explanatory — not a Microsoft or CIS standard)

L0 UNKNOWN	L1 BASIC	L2 MANAGED	L3 MONITORED	L4 CONTINUOUS
No controls confirmed	MFA and defaults active	Baseline + Conditional Access	Score + risk reviewed	Automated drift detection

Microsoft 365 is not insecure by default — but it is not securely configured for every business by default.

MICROSOFT 365 SECURITY REVIEW CHECKLIST

Mark each control: DONE ~ Partial ? Unknown

1 AUTHENTICATE — Identity

[ ] MFA enforced for all users
[ ] Authentication methods reviewed
[ ] Admin accounts use stronger auth (passkey/FIDO2)
[ ] Legacy authentication blocked where feasible
[ ] Break-glass accounts documented and secured

2 LIMIT — Privileged Access

[ ] Global Administrators reviewed and minimised
[ ] Daily and admin accounts separated
[ ] Standing privilege minimised (PIM considered)
[ ] Former suppliers removed from privileged roles
[ ] External delegated access reviewed

3 CONTROL — External Sharing

[ ] SharePoint sharing level reviewed
[ ] OneDrive sharing level reviewed
[ ] Teams guest access reviewed
[ ] Guest accounts periodically reviewed
[ ] Anonymous links controlled or disabled

4 TRUST — Devices

[ ] Supported OS versions required
[ ] BitLocker / disk encryption verified
[ ] Defender endpoint protection active
[ ] Device compliance defined and enforced
[ ] Mobile device access explicitly decided

5 RECORD — Audit Logging

[ ] Purview Audit status verified
[ ] Retention period understood
[ ] Admin changes can be investigated
[ ] Sign-in activity reviewed
[ ] Critical events alert a named owner

6 STANDARDISE — Baseline

[ ] Identity settings documented
[ ] Exchange security documented
[ ] SharePoint / OneDrive settings documented
[ ] Teams security documented
[ ] Exceptions documented with justification

7 REVIEW — Monitoring

[ ] Secure Score reviewed quarterly
[ ] Risky users reviewed and remediated
[ ] Risky sign-ins reviewed
[ ] Admin role changes reviewed
[ ] Corrective actions tracked and assigned

SELF-ASSESSMENT GUIDE

GREEN — Reviewed and controlled

AMBER — Partial or not recently reviewed

RED — Unknown or uncontrolled

RELATED GUIDES

> Microsoft Secure Score Review Checklist
> Microsoft Passkey Readiness Checklist
> Connected Application Access Review