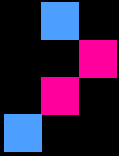


Microsoft 365 Security Checklist



Initial
TECH

Overview

Use this plain-English checklist to harden your Microsoft 365 tenant. It aligns with Microsoft guidance (Baseline Security Mode, Secure Score), CISA SCuBA baselines, and NCSC cloud security advice. Start with the Quick Wins, then work section-by-section, recording evidence as you go.

How to use this checklist

- 1) Sign in to the Microsoft 365 admin and Defender portals.
- 2) For each section, complete the tasks, tick Status, and paste screenshots/links under Evidence.
- 3) Use Secure Score to track progress and prioritise actions.
- 4) Recheck quarterly or when staff/roles/apps change.

Quick Wins (do these first)

- Turn on Multi-Factor Authentication (MFA) for all users and admins (prefer Authenticator/passkeys).
- Block legacy (basic) authentication.
- Apply Preset security policies (Standard or Strict) in Defender for Office 365.
- Enable Microsoft Baseline Security Mode (BSM) and review impact simulation.
- Check Microsoft Secure Score and start the top-impact improvements.

1. Identities, MFA & Admin safety

Protect accounts first. Enforce MFA, minimise admin privileges, and use just-in-time elevation.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enforce MFA for ALL users and admins	Use Conditional Access or security defaults; prefer Authenticator app or passkeys.		
Create two cloud-only break-glass accounts	Use *.onmicrosoft.com addresses with strong MFA; store credentials offline.		
Remove unnecessary Global Admins	Use least privilege; manage with Privileged Identity Management (PIM) for just-in-time access.		
Require MFA and compliant devices for admin roles	Conditional Access: require MFA + compliant/Hybrid-joined devices for admin sign-ins.		
Monitor risky sign-ins	Use Entra ID Protection and Secure Score improvements to address leaked credentials.		

2. Conditional Access (Zero Trust)

Apply risk-based access. Require MFA, block unknown locations, and limit access on unmanaged devices.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Block legacy authentication	Create a CA policy to block “Other clients/Exchange ActiveSync”; start in Report-only then enforce.		
Require MFA for all apps	Baseline policy: All users → All cloud apps → Grant access with MFA.		
Block high-risk sign-ins	Use risk-based CA policies (requires Entra ID P2) to block sign-ins flagged as high risk.		
Restrict from countries you don’t do business in	Location CA policy: block sign-ins from unexpected geographies.		
Limit access on unmanaged devices	Use session controls (disable download, require web-only) for unmanaged devices.		

3. Defender for Office 365 (email & collaboration)

Use Preset policies and fine-tune anti-phishing, Safe Links, and Safe Attachments. Block risky behaviours.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Apply Preset security policies (Standard/Strict)	Enable in Microsoft Defender; cover Safe Links, Safe Attachments, Anti-Phishing, Anti-Spam.		
Block automatic external forwarding	Outbound spam policy: block auto-forward; allow only documented exceptions.		
Enable Safe Links (time-of-click URL scanning)	Turn on Safe Links for email and Office apps; disallow click-through on warnings.		
Enable Safe Attachments (sandboxing)	Enable for all users; choose dynamic delivery/replace; review quarantine regularly.		
Set impersonation protection for execs/brands	Configure anti-phishing policies with mailbox intelligence and impersonation protection.		
Use Configuration analyzer regularly	Compare custom policies with Standard/Strict baselines to catch drift.		

4. SharePoint, OneDrive & Teams (data sharing)

Reduce exposure. Enforce HTTPS, control external sharing, and use sensitivity labels/DLP.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Review and tighten external sharing	Default to “Existing guests only”; require owner approval and expiration.		
Label and protect sensitive data	Use Purview sensitivity labels and DLP to stop oversharing of confidential data.		
Disable custom scripts where not needed	Harden SharePoint/OneDrive settings; restrict anonymous sharing.		
Enable versioning and retention	Keep file versions and apply retention to recover from ransomware or mistakes.		

5. Email authentication & monitoring

Stop spoofing and improve deliverability with SPF, DKIM, DMARC; monitor Secure Score.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Publish and align SPF/DKIM/DMARC	Configure records and policies to reject spoofed mail; monitor alignment reports.		
Review Secure Score weekly	Use Defender portal to prioritise and assign improvement actions; track trends.		

6. Apps & consent (reduce shadow risk)

Require admin consent for third-party apps to access files/sites; review app permissions regularly.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enable admin consent workflows	Prevent users from granting risky app permissions; route requests to admins.		
Audit enterprise apps & service principals	Remove unused apps; restrict high-privilege consents.		

7. Backup & recovery readiness

Prepare to recover fast. Use 3-2-1-1-0 for backups and leverage M365 versioning/retention.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Adopt 3-2-1-1-0 backups with one immutable/offline copy	Keep three copies on two media, one offsite, one immutable; verify restores (zero errors).		
Enable OneDrive/SharePoint versioning & File Restore	Ensure file versioning (≥ 500) and File Restore are enabled to rollback ransomware edits.		
Test mailbox/file restores quarterly	Restore sample items and measure recovery time (RTO/RPO).		

8. Operations, logging & evidence

Turn on auditing, keep logs, and prove compliance.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enable unified audit log	Turn on audit logging in Purview; confirm event coverage.		
Store evidence for changes	Save policy screenshots/links and change tickets to the Evidence register.		
Document exceptions & compensating controls	Minimise scope; review quarterly.		

Action plan (next steps)

Action	Owner	Due date	Resources	Status

References

- Microsoft Baseline Security Mode (GA Nov 2025)
- Microsoft Secure Score overview and usage
- Conditional Access planning and legacy auth blocking
- Defender for Office 365 recommended Standard/Strict policies
- CISA SCuBA baselines & ScubaGear assessment tool
- NCSC cloud security guidance (SaaS/M365 hardening)
- Microsoft 365 ransomware protections (versioning, retention)
- 3-2-1-1-0 backup strategy (immutable copy, verification)