CollabPoint

MICROSOFT SOLUTIONS PARTNER

SECURITY & COMPLIANCE · FIELD GUIDE

The Microsoft 365 Security Baseline

20 controls examiners, auditors, and cyber-insurers expect to see — the hardened configuration standard Microsoft 365 does **not** ship with by default.

For mid-market & regulated organizations

Entra · Defender · Purview · Intune

01 Identity — the new perimeter

Most breaches start with a sign-in. Identity controls are the highest-leverage baseline and where examiners look first.

- [ ] ID-01 CRITICAL

Phishing-resistant MFA enforced for all users

Move beyond SMS/app codes to passkeys, Windows Hello, or FIDO2 for admins and, over time, everyone. **Microsoft Entra ID · Authentication methods**

- [ ] ID-02 CRITICAL

Legacy authentication blocked

Legacy protocols bypass MFA entirely — the single most common way MFA gets defeated. **Entra Conditional Access**

- [ ] ID-03 CRITICAL

Conditional Access baseline in place

Require compliant devices, block risky sign-ins, and gate access by user, app, and risk. **Entra Conditional Access**

- [ ] ID-04 CRITICAL

Privileged roles under just-in-time control

No standing global admins — activate elevated roles only when needed, with approval and logging. **Entra Privileged Identity Management (PIM)**

- [ ] ID-05 HARDENING

Break-glass accounts configured and monitored

Two excluded emergency accounts with alerting, so a Conditional Access mistake can’t lock you out. **Entra ID · emergency access**

02 Email & collaboration

Email is still the top attack vector. These close the gaps default tenants leave open.

- [ ] EM-01 CRITICAL

Defender for Office 365 Safe Links & Safe Attachments on

Detonate attachments and rewrite URLs to catch phishing and malware at click time. **Microsoft Defender for Office 365**

- [ ] EM-02 CRITICAL

Anti-phishing & impersonation protection tuned

Protect executives and your domain against spoofing and business email compromise. **Defender for Office 365 · anti-phishing**

- [ ] EM-03 CRITICAL

SPF, DKIM, and DMARC published and enforcing

Authenticate your outbound mail so attackers can’t spoof your domain — and move DMARC to reject. **Exchange Online · DNS**

- [ ] EM-04 HARDENING

External sharing controls set for SharePoint & Teams

Default sharing is often wide open — scope it to what the business actually needs. **SharePoint Online · Teams governance**

03 Data protection

Protect the data itself, so a leaked file is still governed and, ideally, encrypted.

- [ ] DP-01 CRITICAL

Sensitivity labels classifying and encrypting data

Protection follows the file across M365, cloud, and endpoints. **Microsoft Purview Information Protection**

- [ ] DP-02 CRITICAL

Data Loss Prevention policies active

Stop sensitive data — PII, financial, health — from leaving through email, chat, or upload. **Microsoft Purview DLP**

- [ ] DP-03 HARDENING

Retention & records policies mapped to obligations

Keep what regulators require, defensibly delete the rest, and be ready for eDiscovery. **Microsoft Purview Data Lifecycle Management**

04 Endpoint

Devices are where identity and data meet — and where ransomware lands.

- [ ] EP-01 CRITICAL

Intune compliance policies enforced

Only healthy, managed, encrypted devices get access — tied back to Conditional Access. **Microsoft Intune**

- [ ] EP-02 CRITICAL

Defender for Endpoint deployed across the fleet

EDR for detection and response on every managed device, not just servers. **Microsoft Defender for Endpoint**

- [ ] EP-03 HARDENING

Disk encryption (BitLocker) enforced and escrowed

A lost laptop shouldn’t be a breach; recovery keys stored centrally. **Intune · BitLocker**

- [ ] EP-04 HARDENING

Attack Surface Reduction rules enabled

Block the common ransomware and macro techniques before they execute. **Defender for Endpoint · ASR rules**

05 Monitoring, response & governance

You can’t defend — or prove compliance for — what you can’t see. Close the loop.

- [ ] MON-01 CRITICAL

Unified audit log enabled and retained

Without it you can’t investigate an incident or answer an examiner. Turn it on and extend retention. **Microsoft Purview Audit**

- [ ] MON-02 CRITICAL

Defender XDR / Sentinel alerting monitored

Correlated detection across identity, email, endpoint, and cloud — with someone watching it. **Microsoft Defender XDR · Sentinel**

- [ ] MON-03 HARDENING

Microsoft Secure Score reviewed on a cadence

A single measurable posture score, trended over time and tied to an owner. **Microsoft Secure Score**

- [ ] MON-04 HARDENING

Access reviews & documented policies in place

Recurring reviews of access plus written, approved security policies — what auditors ask for first. **Entra ID Governance · policy set**

Not sure how many of these you actually have?

We run a fixed-scope Microsoft 365 security assessment for mid-market teams — every control below checked against your live tenant, with a prioritized remediation plan you can hand to your board or examiner.

0–8 ✓	9–15 ✓	16–20 ✓
Material gaps — prioritize identity first	Solid base, close the hardening gaps	Exam- and insurer-ready posture

Book a 30-minute intro call →