

Microsoft 365 Business Premium Setup Checklist

14 steps to turn on the security you already pay for. Order matters: start with identity and email.

For: small business owners and office managers

Plan: Microsoft 365 Business Premium

Business: _____ Completed by: _____ Date: _____

Identity: who can sign in

- ☐ **1 Turn on MFA for everyone.** Use security defaults, or switch to Conditional Access (included with Business Premium). Turn security defaults off only when your Conditional Access policies are ready to replace them. No exceptions for "the boss." Done ____/____
- ☐ **2 Lock down admin accounts.** Keep Global Admins to fewer than five, use separate admin accounts for admin work, and keep two secured emergency ("break-glass") accounts. Done ____/____
- ☐ **3 Block legacy authentication.** Old sign-in methods can't do MFA, and attackers love them. Done ____/____

Email: stop phishing and spoofing

- ☐ **4 Apply Defender for Office 365 preset security policies (Standard or Strict).** Turns on Safe Links, Safe Attachments, and anti-phishing. Add owners, partners, and key vendors to impersonation protection. Done ____/____
- ☐ **5 Set up SPF, DKIM, and DMARC for your email domain.** Makes it much harder for criminals to send email as you. Done ____/____

Devices: laptops and phones

- ☐ **6 Enroll devices in Intune.** Require encryption, a screen lock, and current updates. Use app protection policies for personal phones. Done ____/____
- ☐ **7 Onboard devices to Defender for Business.** Check the security dashboard regularly. Done ____/____
- ☐ **8 Require compliant devices for access to email and files.** Set this with Conditional Access. Done ____/____

Data: files, sharing, and records

- ☐ **9 Create a few simple sensitivity labels and a DLP policy.** For example: Public, Internal, Confidential, plus a DLP policy for the sensitive data you handle. Done ____/____
- ☐ **10 Tighten sharing in SharePoint and OneDrive.** Turn off or limit "anyone with the link" sharing. Done ____/____
- ☐ **11 Turn on archiving and retention policies.** Confirm audit logging is on. Done ____/____

People and upkeep

- ☐ **12 Train your people.** Turn on the Report phishing button and run regular awareness training. Add phishing simulations if you license Defender for Office 365 Plan 2. Done ____/____
- ☐ **13 Review Microsoft Secure Score monthly.** It shows what's set up, what isn't, and what to fix next. Done ____/____
- ☐ **14 Have a backup and recovery plan for your Microsoft 365 data, and test it.** Done ____/____

Go slow with Conditional Access. Some of these settings, like Conditional Access, can lock people out if they're set up wrong. Try new policies in report-only mode or on a small test group first, and leave your emergency admin accounts out of any policy that blocks or restricts sign-in.

Want help getting it right?

Hawkcrest Cyber can set this up and check it for you. Cory Zaner, CISSP, CISM. Houston-area cybersecurity architect and U.S. Air Force veteran.

hawkcrestcyber.com/#request

Based on "One Subscription, Your Whole Security Stack" (Hawkcrest Cyber, October 2026). Feature availability and Microsoft admin menus can change, so check Microsoft's current documentation.

Microsoft, Microsoft 365, Defender, Entra, Intune, and Purview are trademarks of the Microsoft group of companies. Hawkcrest Cyber is an independent consultancy and is not affiliated with Microsoft.