SOURCEPASS MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

# Microsoft 365 Hardening Checklist

Sourcepass Center of Excellence for Microsoft | May 2026

## WHY M365 HARDENING MATTERS

**Microsoft 365 is the backbone of modern business productivity — and a prime target for cyber threats. Out-of-the-box, M365 ships with sensible defaults, but a well-hardened tenant requires deliberate configuration across identity, endpoints, email, data, and monitoring.**

**This guide walks through the essential steps every organization should take to dramatically reduce its attack surface, meet compliance obligations, and build a resilient security posture — all within the Microsoft ecosystem.**

## STEP 1 Get the Right Licensing

Effective security hardening starts with the right foundation. Microsoft 365 Business Premium or Microsoft 365 E3 are the minimum recommended licenses for most small-to-mid-sized organizations, as they unlocks the core security toolset needed for the steps in this guide. Without the right licensing, critical controls simply are not available.

Business Premium and Microsoft 365 E3 include, among other capabilities:

- Entra ID P1 — Conditional Access, identity protection, and hybrid identity management
- Microsoft Intune — Cloud-based device management and policy enforcement
- Defender for Office 365 P1 — Advanced email and collaboration threat protection
- Defender for Endpoint P1/Defender for Business — Advanced Endpoint EDR and threat protection

## STEP 2 Run a Security Assessment

Before making changes, understand where you stand. A security assessment identifies gaps across your identity, email, endpoint, and data layers — giving you a prioritized roadmap rather than a random checklist. Microsoft's Secure Score is a great starting point, but a hands-on review by an experienced partner provides deeper context. Focus on pragmatic security changes that drive tangible security improvements.

As part of your initial cleanup, remove or disable dormant user accounts and devices in Entra ID and Intune. Stale accounts are active attack vectors, and they inflate noise in reporting, making it harder to tune policies accurately.

SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

# Microsoft 365 Hardening Checklist

Sourcepass Center of Excellence for Microsoft | May 2026

## STEP 3 Enable MFA for All Users

Enabling Multi-Factor Authentication (MFA) for every user is the single highest-impact security step you can take. Studies consistently show that MFA blocks over 99% of automated credential attacks. Prioritize phishing-resistant methods such as the Microsoft Authenticator app (passwordless push) and FIDO2 security Passkeys over SMS-based codes.

Pair MFA deployment with a solid Conditional Access policy framework. We recommend reviewing our article on the Top 10Conditional Access Policies Every Tenant Should Have, which includes blocking legacy authentication protocols — a common attacker bypass for MFA controls.

## STEP 4 Dial In SPF, DKIM, and DMARC

Email authentication records — SPF, DKIM, and DMARC — are the foundation of phishing and spoofing protection. SPF defines which mail servers are authorized to send on behalf of your domain; DKIM cryptographically signs outbound messages; and DMARC ties them together with a policy that instructs receiving mail servers what to do with messages that fail authentication.

We recommend using a solution such as EasyDMARC for visibility and reporting. DMARC reporting gives you a real-time view of legitimate vs. fraudulent sending on your domain, enabling you to move from a "monitor" policy to a "reject" policy with confidence — stopping domain spoofing dead in its tracks.

## STEP 5 Configure Defender for Office 365

Defender for Office 365 Plan 1 (included in Business Premium and M365 E3) provides layered protection for email and collaboration tools. Properly tuned anti-phishing, anti-spam, and anti-malware policies address the most common attack vectors targeting organizations today. Safe Links and Safe Attachments add real-time detonation and URL scanning that go well beyond basic spam filtering.

Apply Microsoft's "Strict" or "Standard" preset security policies as a baseline, then customize based on your assessment findings and operational requirements. Regularly review quarantine activity and false negative/positive logs to keep policies well-tuned.

SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

# Microsoft 365 Hardening Checklist

Sourcepass Center of Excellence for Microsoft | May 2026

## STEP 6 Enable Mailbox Auditing and Audit Logging

You cannot investigate what you cannot see. Enabling unified audit logging and mailbox auditing ensures that critical actions — sign-ins, mail access, permission changes, file access — are recorded and available for investigation. This is a prerequisite for any meaningful incident response effort and is often required for regulatory compliance.

Audit log retention policies should align with your compliance requirements. Ensure that logs are retained for a sufficient period (90 days minimum; longer for regulated industries) and are regularly reviewed or ingested into a SIEM or MDR platform.

## STEP 7 Enable Microsoft Defender for Business

Microsoft Defender for Business — included in Microsoft 365 Business Premium — or Microsoft Defender for Endpoint —included in Microsoft 365 E3 is one of the most capable Endpoint Detection and Response (EDR) solutions available, consistently recognized by independent analysts. It provides continuous endpoint monitoring, automated attack disruption, vulnerability management, and threat analytics across Windows, macOS, iOS, and Android devices.

Onboard all devices to Defender for Endpoint and review the threat and vulnerability management dashboard regularly. Automated remediation settings can significantly reduce the time-to-respond for commodity threats without requiring manual intervention.

## STEP 8 Build Out Intune Configurations and Deploy Autopilot

Microsoft Intune gives you centralized control over device configuration, update management, and security policy enforcement across your entire device fleet — regardless of whether devices are on-premises or remote. Security baselines in Intune provide a Microsoft-recommended starting configuration that can be deployed in minutes.

Windows Autopilot streamlines device provisioning, ensuring every new device is enrolled, configured, and secured automatically — eliminating manual setup and reducing the risk of misconfigured endpoints entering your environment.

SOURCEPASS MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

# Microsoft 365 Hardening Checklist

Sourcepass Center of Excellence for Microsoft | May 2026

## STEP 9 Require Compliant Device Access

Requiring that only Intune-compliant devices can access sensitive Microsoft 365 resources is one of the most powerful access controls available in the Microsoft ecosystem. By combining Entra ID Conditional Access with Intune compliance policies, you ensure that even authenticated users cannot reach corporate data from unmanaged or non-compliant devices.

Define compliance baselines that include OS version requirements, encryption enforcement, antivirus status, and screen lock policies. Roll out access requirements in stages — starting with high-sensitivity workloads — to minimize user disruption while progressively raising the security bar.

## STEP 10 Deploy DLP Policies and Sensitivity Labels

Data Loss Prevention (DLP) policies and Microsoft Purview Sensitivity Labels work together to protect your most sensitive information. DLP policies detect and block the inappropriate sharing of sensitive data — such as financial records, PII, or health information — across email, Teams, SharePoint, and endpoints.

Sensitivity labels classify and protect documents and emails with persistent encryption and access controls that travel with the content, even outside your organization. Start by locking down SharePoint external sharing settings and defining a label taxonomy that aligns with your data classification requirements before broad deployment.

## Extra Credit: Advanced Security Capabilities

**Organizations that have completed the core hardening steps above and are ready to advance their security posture should consider the following additional investments:**

### Defender Suite & Microsoft Purview (Advanced Add-ons)

Adding the Defender for Office 365 P2, Defender for Identity, and the full Microsoft Purview suite unlocks enterprise-grade capabilities such as Privileged Identity Management (PIM), risky sign-in and risky user policies, advanced data governance, Copilot data protection controls, and a broad range of compliance and insider-risk management tools.

SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

# Microsoft 365 Hardening Checklist

Sourcepass Center of Excellence for Microsoft | May 2026

## 24/7 Managed Detection & Response (MDR)

Even the best-configured tenant benefits from around-the-clock human monitoring. A 24/7 MDR solution provides peace of mind by ensuring that threats detected after business hours are investigated and contained quickly — dramatically reducing dwell time and the blast radius of any incident.

## Ready to Get Started?

**The Sourcepass Microsoft Center of Excellence team specializes in M365 security assessments, hardening engagements, and ongoing managed security services. Reach out to your Sourcepass account team or visit sourcepassmcoe.com to schedule a complimentary discovery call.**