

Microsoft 365 Security Checklist for Small Businesses

Cambium Data | 6542 S 118th St, Omaha, NE 68137 | (402) 514-3200 | cambiumdata.com

1. Sign-in

☐	MFA required for every user (security defaults or Conditional Access)	Owner / date
☐	Shared, service and old accounts included or disabled	Owner / date
☐	Prefer phishing-resistant MFA, such as FIDO2 security keys or passkeys; use stronger methods where supported and avoid SMS when practical	Owner / date

2. Administrator accounts

☐	Separate admin accounts, not used for daily email	Owner / date
☐	Minimize Global Administrator assignments; use least-privilege admin roles	Owner / date
☐	MFA on every admin account	Owner / date
☐	At least two cloud-only emergency access accounts created, securely stored, excluded from restrictive Conditional Access policies, and tested regularly	Owner / date

3. Legacy sign-in

☐	Legacy/basic authentication blocked	Owner / date
☐	Sign-in logs checked for legacy protocols	Owner / date

4. Email

☐	Anti-phishing, anti-spam, anti-malware policies reviewed	Owner / date
☐	Safe Links and Safe Attachments configured where licensed; verify coverage and policy settings for all intended users	Owner / date
☐	SPF, DKIM and DMARC set for every sending domain	Owner / date
☐	External sender warning on	Owner / date
☐	Auto-forwarding to outside addresses blocked	Owner / date

5. Sharing

☐	"Anyone" links limited or disabled	Owner / date
☐	Expiration configured for Anyone links and guest access where supported and appropriate	Owner / date
☐	Teams guests reviewed	Owner / date

6. Devices

☐	Supported devices enrolled in Intune; compliance requirements enforced through Conditional Access where licensed and appropriate	Owner / date
☐	BitLocker on Windows laptops	Owner / date
☐	Remote wipe available for phones	Owner / date

7. Logging and alerts

☐	Microsoft Purview auditing enabled and verified; review retention requirements and available audit features	Owner / date
☐	Alert policies reviewed and sent to a monitored mailbox	Owner / date

☐	Secure Score reviewed; top actions planned	Owner / date
--------------------------	--	--------------

8. Backup

☐	Independent backup covering Exchange Online, OneDrive, SharePoint, and Teams data; verify coverage, retention, and restore capabilities	Owner / date
☐	Test restore done and dated	Owner / date

9. People

☐	New-hire checklist (MFA and licenses day one)	Owner / date
☐	Leaver checklist: block sign-in promptly, revoke active sessions, remove or transfer access and credentials as appropriate, and apply the mailbox retention or delegation process	Owner / date

10. Training

☐	Regular security awareness training	Owner / date
☐	Phishing simulations and a way to report suspicious email	Owner / date

Sources: Microsoft Learn documentation on [Microsoft Entra security defaults](#), [administrator roles](#), [emergency access accounts](#), [legacy authentication](#), [email authentication](#), [Microsoft Secure Score](#), and [Microsoft 365 data protection](#); CISA guidance on [multifactor authentication](#).

Full guide: cambiumdata.com/insights/microsoft-365-security-checklist/