

Microsoft 365 Security Checklist

A practical, vendor-aware review for growing organisations. Use the boxes to record whether each control is in place, partly in place, or requires action.

Identity and privileged access

☐	Multi-factor authentication is required for every user.	Yes / Partly / No
☐	Administrator accounts are separate from everyday user accounts.	Yes / Partly / No
☐	Global Administrator and other privileged roles are reviewed regularly.	Yes / Partly / No
☐	Legacy authentication is blocked unless a documented exception exists.	Yes / Partly / No
☐	Dormant, leaver and guest accounts are removed or disabled promptly.	Yes / Partly / No

Access and device controls

☐	Conditional Access policies have been tested and applied proportionately.	Yes / Partly / No
☐	Only supported, encrypted and appropriately managed devices access business data.	Yes / Partly / No
☐	Mobile-device and bring-your-own-device rules are documented.	Yes / Partly / No
☐	Operating systems, browsers and applications receive timely security updates.	Yes / Partly / No
☐	Local administrator access is restricted and controlled.	Yes / Partly / No

Email, collaboration and data

☐	Anti-phishing and impersonation protection covers senior and finance users.	Yes / Partly / No
☐	External forwarding, anonymous sharing and guest access are controlled.	Yes / Partly / No
☐	SharePoint, Teams and OneDrive sharing defaults match business risk.	Yes / Partly / No
☐	Retention and deletion requirements are defined for important information.	Yes / Partly / No
☐	Sensitive information is identified and protected where proportionate.	Yes / Partly / No

Recovery and assurance

☐	Critical Microsoft 365 data has an agreed recovery approach.	Yes / Partly / No
☐	Administrative and security alerts are reviewed by a named owner.	Yes / Partly / No
☐	Sign-in, audit and incident evidence is retained for an appropriate period.	Yes / Partly / No
☐	Recovery and account-compromise procedures have been tested.	Yes / Partly / No
☐	Existing Microsoft licences are reviewed before overlapping tools are purchased.	Yes / Partly / No

Priority actions

1. _____
2. _____
3. _____

This checklist is general guidance, not legal, regulatory or security assurance. The appropriate controls depend on your organisation, risks, contracts and regulatory obligations.