



Microsoft Secure Score checklist

Use this to lift Secure Score with controls that are actually on — not a number you chase.

Work top-down. Identity first, then email, then devices and data.

Tick only what is enforced. Name a break-glass account before tightening Conditional Access.

IDENTITY

- ☐ MFA required for all users, including admins
- ☐ Legacy authentication blocked
- ☐ Standing Global Administrators kept small and named
- ☐ Privileged roles use just-in-time access (PIM) where licensed
- ☐ User consent for applications restricted
- ☐ Guest access is deliberate — not the tenant default

EMAIL AND COLLABORATION

- ☐ Defender for Office 365 policies on (Safe Links / Safe Attachments where licensed)
- ☐ Anti-phishing policy covers all users, not only a pilot group
- ☐ External sharing in SharePoint and OneDrive is constrained
- ☐ Mailbox auditing and unified audit log are enabled

DEVICES AND DATA

- ☐ Devices that access company data are enrolled or app-protected
- ☐ BitLocker / encryption required for Windows where Intune is in play
- ☐ Sensitive data has a basic Purview / DLP starting point if you handle it

GOVERNANCE

- ☐ Secure Score is reviewed on a cadence, with an owner
- ☐ Changes are recorded (what was switched on, and why)
- ☐ The score is a by-product of the controls — not the target