



ISO 27001 Staff Awareness

A practical introduction to ISO 27001 and what it means for your day-to-day work. One-page summary.

The 10 things to remember

- 1 ISO 27001 specifies a management system, the ISMS, covering people and processes as well as technology.
- 2 Every control protects confidentiality, integrity, or availability; good security balances all three.
- 3 Controls are chosen by risk assessment, which is why rules differ between roles and organisations.
- 4 Know where your policies live: acceptable use, access control, classification, clear desk and clear screen.
- 5 Lock your screen every time you step away, and lock sensitive papers away when you leave.
- 6 Never share credentials, and never approve an MFA prompt you did not trigger.
- 7 Keep work in approved locations so it is backed up, and never adopt unapproved tools quietly.
- 8 Everyone badges through every door; challenge or report tailgaters and unescorted strangers.
- 9 Report events, weaknesses, and honest mistakes promptly; when in doubt, report.
- 10 Answer auditors honestly, never guess, and never polish or invent records.