M365 Security Baseline Checklist

18 controls for IT-light service businesses

LM-09 | Secure | FC-04 Security Assessment

Quick baseline for Microsoft 365 - MFA, conditional access, legacy auth, admin roles, sharing, and audit logging before customers or insurers ask.

Identity & access

- [ ] MFA enforced for all users - no permanent exceptions
- [ ] Conditional Access policies block legacy authentication
- [ ] Global Administrator count minimised; PIM or just-in-time where possible
- [ ] Break-glass accounts documented and excluded from CA only as required
- [ ] Guest access reviewed quarterly; default sharing links restricted

Email & data

- [ ] Outbound spam and phishing policies enabled with reporting mailbox
- [ ] Safe Links and Safe Attachments on for priority users at minimum
- [ ] External sharing defaults set to least privilege for SharePoint/OneDrive
- [ ] Retention labels applied to contracts and financial records

Brisbane, Australia | Australia-wide delivery

hello@northark.ai

- [ ] DLP rules considered for credit cards, TFNs, or client PII in email

Monitoring & response

- [ ] Unified audit log enabled and retained per policy
- [ ] Alert rules for impossible travel, mass download, or admin role changes
- [ ] Incident response contact list includes someone who can revoke sessions
- [ ] Quarterly access review for admin roles and app registrations
- [ ] Secure Score reviewed monthly with top three actions assigned owners

Need expert review? Book a free discovery call at northark.ai/book