Your IT security. Checked. Not assumed.

I want evidence, not a guess. Review this with your IT owner or provider. Mark one status per item and assign an owner. - D.O.N.N.A.

Company _____ Review date _____

Verified = evidence checked. Needs work = a gap. Unsure = verify before relying on it.

01 Require multifactor authentication

Cover email, admin and key business accounts. Prefer passkeys or security keys where supported.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

02 Protect password and MFA recovery

Verify identity before resets. Keep recovery methods current and emergency admin access protected.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

03 Limit powerful access

Give people only the access they need. Use a separate admin account for privileged work.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

04 Close access when people leave

Disable accounts, revoke sessions and remove group/app access. Preserve business information.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

05 Know your devices and applications

Keep an inventory with an owner for each system. Include personal devices used for business.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

06 Verify updates actually succeed

Check operating systems, browsers and apps. Resolve failed updates and replace unsupported software.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

Your first priority

_____

Due date _____ Evidence location / reference _____

Keep the completed checklist private. Never record passwords here.

Keep the foundations working.

Complete the remaining checks. Then decide who keeps checking.

07 Keep device protection working

Confirm encryption, endpoint protection and firewalls are enabled and reporting on business devices.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

08 Review who can see business information

Check folders, shared drives, groups and guests. Remove access that no longer has a business purpose.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

09 Protect business email

Check phishing protections and SPF, DKIM and DMARC domain authentication with your provider.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

10 Independently verify sensitive requests

Confirm payment changes and access requests using a known contact method. A familiar voice is not proof.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

11 Set rules for AI tools

Approve tools, data use and connected-system access. Review sharing permissions before introducing AI.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

12 Prove you can recover

Back up critical information and test restores. Name an incident owner and keep a usable response plan.

☐ Verified ☐ Needs work ☐ Unsure Owner: _____

A practical review rhythm

Continuously, where supported: security alerts and failed protections.
Every joiner, role change or leaver: accounts, access, groups and sessions.
Daily / weekly: unresolved alerts, failed updates, backups and offline devices.
Monthly: admin access, inactive accounts, external sharing and connected apps.
Quarterly / after major changes: restore tests, incident exercises and staff guidance.

Next review _____ Review owner _____

Read the guide & sources

Need a starting point? Get your IT Health Score.

Adapt to your risk. This checklist is not a compliance certification or a security guarantee.

Keep the completed checklist private. Never record passwords here.