Company Cybersecurity Policy Readiness Audit Checklist

Use the following checklist to assess your organization's current cybersecurity governance maturity.

Check each item honestly.

Core Policy Controls

☐ We have a documented password and authentication policy.
☐ Multi-factor authentication is mandatory across critical business platforms.
☐ Shared account credential handling is formally controlled.
☐ Employees use approved secure credential storage methods.
☐ We have a written acceptable use/device usage policy.

Employee Behaviour Governance

☐ Unauthorised software installation is prohibited by policy.
☐ Personal cloud file transfer restrictions are documented.
☐ USB/removable media usage is governed.
☐ AI tool usage with business data is addressed internally.
☐ Employees know exactly how to report suspicious emails.

Remote Work and Mobility Controls

☐ We have a formal remote work cybersecurity policy.
☐ Personal device usage rules are clearly defined.
☐ Mobile phone business access protections are documented.
☐ Lost/stolen device reporting expectations are immediate and clear.

Access Governance

☐ Least-privilege access principles are actively applied.
☐ Employee onboarding/offboarding access controls are standardised.
☐ Shared cloud folder permissions are reviewed periodically.
☐ Administrative account access is tightly limited.

Vendor and Third-Party Governance

☐ New SaaS/vendor approvals include security review.
☐ Third-party access permissions are reviewed on a recurring basis.
☐ Vendor incident escalation responsibilities are assigned.

Incident and Recovery Readiness

☐ We have a documented internal cyber incident reporting chain.
☐ Employees understand what events must be escalated immediately.
☐ Backup schedules and retention are formally documented.
☐ Backup restoration is tested periodically.
☐ Cybersecurity policies are reviewed at least annually.

SCORING YOUR RESULTS

20–25 boxes checked = STRONG MATURITY

Your organisation has meaningful internal cyber governance foundations and is operating with stronger digital discipline than most small to mid-sized businesses.

12–19 boxes checked = MODERATE EXPOSURE

You likely have partial controls in place, but meaningful policy inconsistency still leaves avoidable human and operational gaps.

0–11 boxes checked = HIGH VULNERABILITY

Your organisation is operating with significant undocumented cyber behaviour, weak accountability, and elevated preventable incident risk.