Security policy starter

A policy is useful only if people can understand it and you can enforce it. This starter covers the basics. Adapt it to how your business actually works and have it approved by whoever is accountable. It is a starting point, not legal advice, so check it against your jurisdiction and sector.

Business

Policy owner

Approved by

Review date

POLICY CLAUSES

1. Scope
This policy applies to everyone who accesses business systems, including employees, contractors, temporary staff and suppliers with remote access. It covers business devices and personal devices used for work.

2. Responsibilities
The owner is accountable for this policy. Managers make sure their teams follow it. Everyone is responsible for reporting suspected incidents, phishing or lost devices promptly and without blame.

3. Acceptable use
Business devices and accounts are for legitimate business use. Do not install unapproved software, disable security controls, share credentials or use business systems for unlawful activity. Limited personal use is acceptable if it does not create risk.

4. Devices and updates
Work devices must have automatic updates, screen locks and disk encryption enabled. Lost or stolen devices must be reported immediately so access can be revoked and the device wiped remotely. End-of-life devices must not hold business data.

5. Accounts and access
Use a password manager and a unique password for every service. MFA is required for email, banking, admin accounts and remote access. Admin accounts are separate from everyday accounts. Access is removed on the last working day when someone leaves.

6. Data and backups
Business data must be stored in approved systems, not personal cloud accounts or unencrypted USB drives. Critical data is backed up automatically, with at least one copy offline or immutable. Restores are tested at least twice a year.

7. Email and payments
Any change to bank details, supplier accounts or payment destinations must be verified by a voice call to a known number. Never rely on email alone. Suspicious messages are reported, not forwarded or deleted quietly.

8. Remote work

Remote access to business systems must use the approved VPN or zero-trust service with MFA. Do not use public Wi-Fi for business systems without protection. Keep devices and paper records out of sight in shared spaces.

9. Incidents

Report suspected incidents immediately to the incident lead. Do not try to investigate alone, delete evidence or contact the suspected attacker. The incident plan sets out who decides, who calls the bank and who communicates.

10. Review

This policy is reviewed at least annually, and after a significant change to staff, systems, suppliers or the way the business works. Changes are recorded and communicated to everyone in scope.

EMPLOYEE ACKNOWLEDGEMENT

- ☐ I have read and understood this policy.
- ☐ I know how to report a suspicious email, lost device or security concern.
- ☐ I understand that reports are encouraged and will not be met with blame.

ACKNOWLEDGEMENT

Name	Role
Signature	Date

REVIEW NOTES

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Printing tips

Use A4 portrait, 100% scale, and turn off headers and footers for the cleanest result. Keep a printed copy somewhere you can reach without email or the shared drive.