03. Access control policy

> **Template.** Part of the open-source AI App Policy Kit, version 1.0. Replace everything in [square brackets], delete what does not apply, and have the person who runs the business approve it. A starting point, not legal advice.

Business	[Business name]
Document owner	[Name and role]
Approved by, and date	[Name], [date]
Next review	[Date, at most 12 months on]

Why this matters

A shared or stolen password is the most common way into a small business's systems. When everyone has their own login with two-step sign-in, a stolen password is not enough, and you can see who did what.

Who it covers

Everyone with access to [Business name]'s apps, source code, cloud accounts, domain and DNS, AI tools, email and payment systems.

The rules

1. **One person, one login.** No shared accounts. Where a system allows only one login, keep its password in the password manager and record who can use it.
2. **Two-step sign-in everywhere it is offered.** It is mandatory for email, the cloud account, the code host, the domain registrar, the password manager and anything holding customer data. Prefer a passkey or an authenticator app to text messages.
3. **Use a password manager.** Passwords are unique, generated and stored in [password manager]. None in documents, chats or notebooks.
4. **Least access.** Each person gets the access their job needs and no more. Admin rights are for the people named below.
5. **Separate admin from everyday use.** Admins use a separate admin account, or raise their rights only for the task.
6. **Protect the root accounts.** The cloud provider's root or owner login, the domain registrar and the code host's owner account each have two-step sign-in, recovery codes stored safely and at least two named people who can recover them.
7. **Joiners, movers, leavers.** Access is given on request from [manager], changed when a role changes and removed on the last working day. Contractors' access has an end date.
8. **Review every [3 or 6] months.** [Policy owner] reads the list of users of each system and removes what is no longer needed.
9. **Machines have their own identities.** Apps, pipelines and AI agents use their own keys or roles with the narrowest rights that work, never a person's login (document 04).

10. **Lock devices.** Laptops and phones used for work lock after [5] minutes, have disk encryption on and are kept updated.

Access register

System	Who has access	Admins	Two-step on?	Last reviewed
Cloud account [provider]	[Names]	[Names]	[Yes]	[Date]
Code host [provider]	[ ]	[ ]	[ ]	[ ]
App admin area	[ ]	[ ]	[ ]	[ ]
Domain and DNS	[ ]	[ ]	[ ]	[ ]
AI tools	[ ]	[ ]	[ ]	[ ]
Email and documents	[ ]	[ ]	[ ]	[ ]

Checklist

- ☐ No shared logins remain, or each one is recorded with its users.
- ☐ Two-step sign-in is on for every system in the register.
- ☐ Two people can recover each root account.
- ☐ Every leaver in the last 12 months was removed on their last day.
- ☐ The register was reviewed on schedule.

References

- NCSC, *Small Business Guide: Cyber Security* and *Cyber Essentials: Requirements for IT infrastructure* (user access control).
- NCSC, *Multi-factor authentication for your corporate online services*.

AI App Policy Kit, version 1.0. © 2026 PugliseWeb LTD, licensed under CC BY 4.0: use it, change it and share it, with credit. The whole kit, and a free Software Health Check of your app against it: https://www.pugliseweb.com/ai-policy-kit