11. Logging and monitoring standard

> **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

Most small businesses learn of a break-in from someone else, weeks later. Logs tell you that something happened, and afterwards, what. Without them you cannot tell the ICO or your customers what was taken. Logs are also where personal data and secrets end up by accident.

Who it covers

Every app and cloud account [Business name] runs, and the AI features inside them.

The rules

1. **Record who did what.** The app logs sign-ins (successes and failures), password and two-step changes, permission changes, exports and deletions of data, and admin actions, each with the time, the user and the address they came from.
2. **Turn on the provider's audit log.** The cloud account, the code host and the identity provider each keep a log of administrative actions. Switch it on and keep it [12] months.
3. **Log AI use.** For each AI request record the time, the user, the feature, the model, the size and cost, and whether a safety rule blocked it. For AI agents, also record each action taken.
4. **Keep personal data and secrets out of logs.** No passwords, keys, tokens, card numbers or full message bodies. Record an id, not a name. If prompts must be kept to investigate problems, keep them separately, with limited access and a short life (document 10).
5. **Keep logs where an intruder cannot erase them.** Send them to a store the app's own login cannot change or delete.
6. **Keep them long enough.** Security logs for at least [90 days, 12 months preferred]. Then they expire automatically.
7. **Alert on what matters.** A person is told at once, by a route they will notice, when one of the events below happens.
8. **Look.** Someone named reads the alerts the same day and reviews the logs for anything odd every [month].
9. **Watch that the app is up.** An outside check calls the app every few minutes and tells someone when it fails.

10. **Keep clocks in step.** All systems use synchronised time, in UTC, so events can be put in order.

Alerts

Event	Tells whom	How	Tested on
Many failed sign-ins for one account or from one address	[Name]	[Phone notification]	[Date]
Sign-in to an admin or root account	[ ]	[ ]	[ ]
A new admin user or access key is created	[ ]	[ ]	[ ]
Large export or deletion of data	[ ]	[ ]	[ ]
Cloud or AI spend above [£] in a day	[ ]	[ ]	[ ]
Error rate or response time above normal	[ ]	[ ]	[ ]
The app is unreachable	[ ]	[ ]	[ ]
Audit logging is switched off	[ ]	[ ]	[ ]
A secret is found in the code	[ ]	[ ]	[ ]

Review record

Date	Reviewed by	Period covered	Anything odd?	Action
[ ]	[ ]	[ ]	[ ]	[ ]

Checklist

- ☐ The audit log is on for the cloud account, the code host and the identity provider.
- ☐ Each alert in the table was triggered on purpose once, and reached a person.
- ☐ A search of the logs for an email address and for a key prefix finds nothing.
- ☐ The app's own login cannot delete its logs.
- ☐ The log review happened on schedule.

References

- NCSC, *Introduction to logging for security purposes*.
- OWASP, *Logging Cheat Sheet*.

AI App Policy Kit, version 1.0. © 2026 PuglieseWeb 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.puglieseweb.com/ai-policy-kit