Calean Tech

Secure AI checklist

Twelve questions to answer before putting AI to work on company data.

Use it before rolling out an AI tool to your team, or before connecting AI to company data. Every “I don’t know” is a work item.

Data

- [ ] Do we know what data the AI will read, and where it comes from?
- [ ] Are personal and confidential data left out, or masked?
- [ ] Does the vendor use our data to train its models? Is that written in the contract?

Access

- [ ] Does the AI see only what the person asking is allowed to see?
- [ ] Are the integration’s credentials temporary and kept in a vault, never in code?
- [ ] Is there a named owner for each AI use?

Use

- [ ] Does the team know what it may and may not paste into an AI tool?
- [ ] Is there an approved tool, so nobody needs a personal account?
- [ ] Do answers that become decisions go through human review?

Record

- [ ] Do we keep who asked what, and when?
- [ ] Can we switch the integration off in minutes if something goes wrong?
- [ ] Do we review this checklist at least every six months?