AI POWER HOUR · CHEAT SHEET

Answering AI questions on security reviews

The six AI questions enterprise buyers ask now, with sample answers. Replace everything in [brackets] with your own details, and only say what's true.

WHAT THEY ASK	HOW TO ANSWER
Which AI tools touch our data?	Name the tools and plans. "We use [Claude Team] and [ChatGPT Business] for internal work. Your data is only processed in [tools], under signed data agreements."
Do those vendors train on our data?	"No. Our AI vendors' business terms prohibit training on customer content, and we've confirmed the settings. [Link to vendor terms.]"
How long is it kept, and where?	Give the retention period and region from each vendor's terms. "[Vendor] keeps data for [X] days and processes it in [region]."
Are they on your subprocessor list, with a DPA?	"Yes. [Vendors] are listed as subprocessors at [link], and we have signed DPAs with each." (Add BAAs if health data is involved.)
Who on your team can use AI with our data?	"Only [roles], on company-managed business accounts. Our AI use policy sets the rules, and personal accounts are not permitted for customer data."
Can your AI agents reach production or our data?	"No agent has production access. Agents run in sandboxes with only the data each task needs, and a person approves anything that sends, deletes or changes records."

Get ready before they ask

1. Pick one approved tool per job, on a business plan.
2. Sign each vendor's DPA. Add a BAA if you touch health data.
3. List your AI vendors on your subprocessor list.
4. Write your one-page AI use policy.
5. Put the short version on a security page on your website.

Start early. SOC 2 audits and vendor agreements take months, not days.

Plain-language glossary

Subprocessor	Any outside company that handles your customers' data for you. If you send customer data to an AI vendor, that vendor is one.
DPA	Data processing agreement: the contract that says how a vendor handles personal data on your behalf.
BAA	Business associate agreement: the health-data version, required under HIPAA in the U.S.
SOC 2	An independent audit of your security practices. Buyers usually ask for the report.