Nucybersec

PRIVATE AI, INSIDE YOUR BOUNDARY

Give this to whoever looks after your systems: your IT provider, your firm administrator, or the person who set up your email. They do not need to have read anything else.

Four questions to ask before any AI tool touches your documents.

Each one is answerable in an afternoon by the people who already run your systems. None of them requires the vendor's cooperation, which is the point. What matters is not whether the answer is yes, but whether it is specific.

01

Can it reach the internet at all?

A good answer describes an absent route rather than a blocked one. In a cloud tenancy there is no gateway or address-translation route out of the network it sits in. On owned hardware there is no connection to check, because there is no cable to one.

02

Where do our documents go when someone asks a question?

A good answer is "nowhere". The model should be reached inside the same boundary the documents already sit in. If any part of the answer involves a copy leaving, that copy is a second custodian of your material.

03

Who can read what we ask it?

A good answer names a key that you hold. Ask specifically whether the vendor could produce your questions and answers if a court asked them to. A vendor who never holds the key has nothing to produce.

04

How would we know if that ever stopped being true?

A good answer is something you can run yourself, on your own schedule, without telling anyone. If verification depends on the vendor sending you a report, you are not verifying, you are being told.

If an answer comes back hedged, that is the finding. These are not trick questions and they do not require a security specialist to ask. A supplier who cannot answer them plainly about their own product is telling you something useful.

Retention promises are policy, and policy has been rewritten by courts in cases the customer was never party to. An architectural answer survives that. A contractual one may not.

Nucybersec LLC

A North Carolina limited liability company. We build retrieval AI that answers from your own documents and cites its sources, running inside a boundary you already control: your own cloud tenancy, or hardware in your own building.