Security posture and technical specification

Centurion is a private AI system that runs on a computer you own, in your building. This sheet states where your data lives, what leaves the machine and where it goes — field by field — so your reviewers can check it rather than take it on trust.

NO COPY TO BREACH

Documents, memory and history are never collected from the machine. What does not exist cannot be stolen, subpoenaed or retained.

NO LOGIN TO ATTACK

One local account, no inbound connection, no portal and no tenancy. There is no remote session to hijack.

NO SERVICE TO SWITCH OFF

It runs on hardware you own, in open formats. It keeps working if we stop existing.

01 What never leaves the building

- Your Soul document, your memory, your projects, your files and your conversation history are stored on your machine and are never replicated to us. There is no support channel into them.
- No account of ours is required for the system to operate, so there is no central store of your content to be breached, subpoenaed or leaked.
- No analytics SDK ships with the software and we operate no telemetry endpoint. Usage statistics are computed and stored locally, for your own `/insights` view.
- Encrypted at rest with LUKS, unlocked by the machine's own TPM — a drive removed from the unit is unreadable, and the machine still restarts unattended after a power cut.

02 What does leave, and where it goes

DESTINATION	WHEN	WHAT IT CARRIES
Your model provider	Every prompt you send	Prompt text only, under that provider's terms. Nothing at all when an on-board model is installed.
Licence server — activate	At activation; after hardware failure	Seven fields, five distinct values. Named in 04.
Licence server — check-in	At most every 30 days, while the licence is live	Eight fields. Named in 04.
Licence server — re-issue	Hardware failure only, on request	Six fields. Named in 04.
Release bucket	Update check and download	The installer and its manifest. No configuration, no usage data.
Phone relay (ours)	Only when used away from your network	The session. It is not a store of your content; on your LAN it is never involved.

> **NOTHING ELSE**
>
> No other outbound traffic is originated by the software. If you would rather verify this than read it, enable outbound logging for a month and compare the tally against this table, field by field.

03 Access and custody

- **No inbound service.** A dedicated firewall zone drops unmatched inbound traffic: no open ports, no allowed services, ssh and mDNS disabled. There is nothing to port-scan and no service to authenticate to.
- **One local account**, protected by the machine passphrase, inside a building you already control.
- **No login surface, so nowhere to add MFA.** A second factor protects a door; this system has none. Where one genuinely belongs is the messaging account in your name that carries the phone interface — enable two-step verification there and put a passcode on the phone. A stolen, unlocked phone is the realistic way in.
- **Our side.** Staff access to licence administration requires TOTP authenticator codes. That is our exposure, not yours — stated because a fair review will ask.
- **A legal demand reaches records that exist.** We hold licence and billing records — the name on the licence, the billing record, the email address, the device fingerprint and the licence history in 04. Those could be compelled, and we would produce the narrowest set the order requires rather than a dataset. Your documents, memory, projects and conversation history could not: they are on your disk and nobody here can read them.
- **For scale.** OpenAI publishes its own tally: in the six months to December 2025 it received 224 non-content demands — subpoenas for name, email, payment and transaction history — and 75 content demands for prompt text and files, disclosing data in 146 and 62 of them respectively. The same two categories were 119 and 26 in the preceding six months, and 29 and 8 a year before that. Those figures exist because there is a central store to demand.
- **Where this weakens, stated plainly.** A cloud-model configuration sends prompt text to that provider, so a demand served on them is a demand on your content, and we cannot answer for their counts or their disclosure decisions. An on-board model removes that party from the chain.
- Add a second user, or expose the machine beyond your LAN, and MFA comes into scope immediately.

04 The licence check, field by field

These are the only automated contacts with our servers. Every field is listed; none of them is content.

REQUEST	FIELDS
`POST /license/activate`	`code · activation_code · hardware_id · machine_fingerprint · install_id · api_key (if configured) · tier`
`POST /license/checkin`	`license_id · install_id · machine_fingerprint · tier · last_state · centurion_version · os_version · nonce`
`POST /license/reissue`	`license_id · token_id · old_fingerprint · new_fingerprint · reason · proof_of_purchase`

> READ THIS PRECISELY
>
> `os_version` is a string of the form `Linux 7.2.11` — system and kernel release only. `nonce` is random per request. Requests identify themselves with the user agent `CenturionBrain/<version>`. There is no hostname, no username and no machine name in any of the three. No files, no prompts, no conversation content, no directory listing, no installed-software inventory.

05 The device fingerprint

A licence has to be bound to something, or one licence serves a thousand machines. It is bound to a single hash derived from the OS-level machine identifier, the board or SMBIOS serial where the hardware exposes one, the operating-system family and the install identifier — and nothing else.

> DELIBERATE OMISSION
>
> The hostname is excluded. It is trivially changed, so including it would make the binding unreliable. The raw identifiers are not transmitted as a machine inventory.

06 Supply chain and updates

- Every artefact publishes a SHA-256 checksum. Verify it before you run anything.
- Linux installers carry an OpenPGP signature on the RPM. The public key ships with the release and its fingerprint is `25CB 4090 1F83 44D3 704F 9A4A C9E7 4757 8FA4 1F8F`.
- Security patches are part of the licence: no support tier to buy in order to stay patched, and no upgrade gate that withholds a fix.
- Release notes name what changed, including security-relevant changes.

07 Third parties

PARTY	ROLE	SEES YOUR CENTURION CONTENT
Vercel	Website and API hosting	No
Supabase	Account, licence and subscription records	No
Stripe	Payment processing	No — card data never reaches us
Resend	Transactional email	No
GoHighLevel	Enquiries and CRM	No
Cloudflare	CDN and edge protection	No
Your model provider	Inference, if you run a cloud model	Prompt text only. Not involved when an on-board model is installed.

08 What we have not done

We hold no SOC 2 report. We hold no ISO 27001 certification. We have not published a third-party penetration test. We are a small company with a small team, and no audit has been commissioned by anyone yet.

If your policy requires either certification before you can approve, that is a real blocker and you should say so rather than let us imply otherwise. What we can evidence instead: every fact in this document, a published checksum and OpenPGP signature for everything you install, and the actual activation request your machine will send, handed to you to read before it goes out.

09 Supply and licence

Centurion Brain — €9,500. The computer, the arrival package and twelve months of licence, updates and support. From month thirteen the licence renews at €50 a month or €600 for the year. Current pricing and inclusions for everything else are published at `1association1ai.com/order`.

It is designed to run as a single-user system. Where a second user or remote access is required, that is a deployment change and it brings authentication requirements with it — raise it before the machine is commissioned, not after.

Centurion AI is a trading name of Adrian Barkus, a sole trader in the United Kingdom.
hello@1human1ai.com · +44 7427 833 508 · 1association1ai.com/en/trust
Verified against the released software, 26 October 2026. When the software changes, this document changes with it.