Security overview

Issued 14 October 2026. Permanent URL: https://reliablecontext.com/security

Reliable Context runs inside your infrastructure, with one database per organization. This overview summarises architecture, data flows, deployment, model routing and the security-review process, as stated on the trust, perimeter, product and guarantees pages. It makes no certification claim.

Architecture

Private sources, licensed feeds and public records enter through one gate, governed by the same five policies: sources, model routing, reader clearance, retention and audit export. One database holds the result. Values leave as an export that an auditor can read on its own.

Each organization runs its own database. There is no shared corpus, no pooled index and no cross-customer model of anything. Two deployments do not share storage, so isolation is a structural property rather than a setting.

Data flows

Material moves in three steps, each governed by a policy you set.

- In: only sources on your permitted list are read. A source whose licence restricts redistribution is read, and every excerpt taken from it carries that restriction wherever it later surfaces.
- Inside: the database for your organization holds the retained evidence and the values read from it. There is no hosted copy of your record.
- Out: every value exports with the sentence it was read from, the source, the locator, the date the source was read and the date the value entered the record. A declared negative exports with what was searched and when.

Deployment in your perimeter

The deployment runs on infrastructure inside the boundary you control. The proposed boundary, network egress and permitted destinations are reviewed against your policies before work starts. Retained evidence belongs inside that boundary.

We do not resell your data, we do not train models on your material, and we do not keep a hosted copy of your record.

Model routing

Which engines may see which class of material is written once as a policy, not settled job by job. Material is classified, each engine has a ceiling, and an engine is never handed material above its ceiling, including on a retry or a fallback. The routing that applied is recorded with each value.

No provider should be inferred from this overview. The permitted route for an engagement, and any provider terms that apply, are given in writing for that engagement.

Reader clearance

You decide who may see which source. A reader who is not cleared for a source does not receive the values resting on it. Those values are labelled blocked, attributed to the source and to the policy that withheld them, and shown in place, so a restriction is never mistaken for an absence of evidence.

Retention and legal hold

Your policy sets how long a retained document and the values read from it are kept, counted from the date each was read. Expiry removes the retained copy and marks every dependent value as no longer reproducible; it does not delete the value and its history. A legal hold suspends expiry for everything in its scope until it is lifted, and is itself recorded with its dates.

Security-review process

Start a review by email to hello@reliablecontext.com, describing the proposed infrastructure boundary, the evidence and source classes, your questionnaire or review topics, and a preferred secure channel for documents. Do not send confidential material in a first email. We reply within two business days.

The response is written for the specific engagement. Topics we answer:

- Deployment topology and organization boundary
- Network egress and permitted destinations
- Model engines and routing by material class
- Access control and reader clearance
- Retention, legal hold and deletion
- Logging and audit export
- Incident notification
- Subprocessors for any hosted part

What this overview does not claim

This site makes no certification claim. Questionnaire answers, applicable provider terms and any hosted-part subprocessors are given in writing per engagement. A generic badge cannot settle what happens to a particular source under a particular policy.