

# SOSA DevOps

Sovereign Systems - AI Disclosure

---

## AI Disclosure -- SOSA DevOps

Effective: 2026-05-15

Applies to: SOSA DevOps desktop application, version 1.0 and later

Provider: Sovereign Systems, Thailand

Contact: ai@sovereignsystems.cc

This document fulfils the transparency obligations that apply to the SOSA DevOps desktop application under the European Union's AI Act (Regulation (EU) 2024/1689), in particular Article 13's transparency requirement for AI systems that interact with natural persons. It is also a plain-language description of how AI works inside the application, written so that any user -- not only EU users, not only legally trained users -- can read it and understand what is happening.

If you have not yet read the Privacy Policy and the Terms of Service, this document depends on them. They define Vault A, Vault B, and the AI Disclaimer; this document references all three and does not repeat the full text.

### 1. Purpose

SOSA DevOps invokes AI Models on your behalf to produce text -- chat responses, retrieval-augmented answers grounded in your indexed documents, and (in future versions) agentic plans. Because you are interacting with an AI system, you are entitled to know:

- \* that AI is in use,
- \* which AI is in use,
- \* where the AI runs,
- \* what is logged,
- \* what your rights are,
- \* and where the system is **\*\*not\*\*** authorised to operate.

This document answers each of those questions for v1.0.

### 2. AI Features in SOSA DevOps

The Software exposes AI through the following features in v1.0:

Local LLM chat (Synapsis module). A conversational interface that sends your prompt to a locally running Large Language Model and renders the response. The Model is one you have pulled through Ollama -- for example Llama 3.1 (Meta), Qwen 2.5 (Alibaba), Mistral (Mistral AI), Phi 3 (Microsoft), Gemma (Google), or another model from the catalog. The Software does not pre-select a Model for you; you choose.

Retrieval-Augmented Generation (RAG). When you have indexed a corpus of documents, the Software embeds each document chunk using a local embedding model -- nomic-embed-text (English-default) or nomic-embed-text-v2-moe (multilingual; supports Thai, Vietnamese,

# SOSA DevOps

Sovereign Systems - AI Disclosure

---

and other Southeast-Asian languages alongside major world languages). At query time, the Software searches the embeddings via a SQLite vec0 nearest-neighbour index, joins the retrieved chunks into a context window, and passes them with your prompt to the LLM. Retrieved chunks are logged to Vault B as rag\_retrieval rows (see Privacy Policy §5).

Persona system. Personas are structured prompt-prefix templates that shape the LLM's tone, role, and constraints. A persona is not a separate AI surface; it is a system message prefix the Software prepends to your prompt before sending it to the LLM. You can create, edit, and delete personas. The Software ships with a default set; replacing them is supported.

Agentic routing pipeline (architecture). The application architecture defines a pipeline -- classify, context, privacy, plan, critic, execute, review, ledger -- for multi-step agent workflows. The architecture is documented in docs/architecture/CHAT\_AGENTIC\_ROUTE.md. Full agentic routing is not wired in v1.0. The pipeline scaffolding exists; the user-facing surface is post-launch. v1.0 chat is single-turn LLM chat (with optional RAG), not multi-step agent execution.

External API providers (deferred). The architecture supports user-keyed external API providers. None are wired in v1.0. The "External Providers" tab shows every provider as Disabled. v1.1+ adds DeepSeek as the first concrete external provider, after which this document will be revised. See §9 for the constraints that will apply when external providers are wired.

## 3. How AI Processing Works

All AI processing in v1.0 happens locally on your device. This is the core architectural commitment of SOSA DevOps and the reason the application can give the privacy guarantees it does.

The processing flow for a typical chat turn is:

1. You type a prompt in the Synapsis chat composer.
2. The Software (in the Tauri webview, written in TypeScript and React) packages the prompt with any persona prefix and any RAG-retrieved context.
3. The packaged payload is sent over a localhost HTTP request (127.0.0.1:11434) to the Ollama runtime that you installed separately.
4. Ollama loads the Model into memory (CPU or GPU, depending on your hardware) and produces a response, streaming tokens back over the same localhost connection.
5. The Software displays the streamed response, and at the end of the turn writes the prompt, the RAG context (if any), and the response to Vault B (interaction-log.jsonl), with the matching cryptographic seals in Vault A (audit-chain.jsonl).

Several properties follow from this flow:

\* **\*\*No prompt or response leaves your device.\*\*** The localhost interface (`127.0.0.1`) is a loopback address; it does not produce a packet on any network. You can verify this

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

with any network monitor.

\* **\*\*No upload, no sync, no telemetry.\*\*** The Software does not transmit your prompts, responses, or RAG context to Sovereign Systems or to any third party. There is no code path in the Software that does this. (See Privacy Policy §3.)

\* **\*\*Models do not learn from you.\*\*** Ollama performs **\*\*inference\*\***, not training. The Model's weights are frozen at the version you pulled; running the Model does not update its parameters. Your prompts are not aggregated, sampled, or fed back to the Model's author for retraining. The same applies to the embedding models used for RAG.

\* **\*\*The application does not pre-process your prompts in a hidden way.\*\*** The only systematic addition to your prompt is the persona prefix you have chosen and the RAG context that you have configured. There is no covert system prompt extracting structured data from your input for any other purpose.

### 4. AI Operation Logging -- Vault A and Vault B

Every AI action the Software performs is logged on your device. This is part of the transparency commitment of the application: you can audit what the application has done in your name, when, and with which Model.

Vault A seals each AI event cryptographically. Per Privacy Policy §4, Vault A entries contain timestamps, event types, character counts, and content hashes -- never readable content. Vault A is the answer to the question "did this happen?" with cryptographic certainty.

Vault B records the readable content of each AI interaction. Per Privacy Policy §5 and the Interaction Log schema (docs/architecture/INTERACTION\_LOG\_SCHEMA.md v1), each row carries the prompt, the response, or the RAG chunks, along with the model name, token counts, and latency. Vault B is the answer to the question "what was actually said?" -- for your eyes, for your model evaluation, for your fine-tuning curation.

The two files are paired. Each Vault B row carries a `linkedAuditSeal` field that contains the hash of its corresponding Vault A entry. You can cross-reference the two: open Vault A to confirm an event happened, then open Vault B to read what it contained.

You access both vaults from the application:

- \* Vault A: `Tools ? Open Audit Vault`
- \* Vault B: `Tools ? Open Interaction Log`

You export Vault B in any of three formats: JSONL (raw v1 schema), TXT (branded transcript), or PDF (branded transcript with integrity certificate). You delete Vault B per session via the type-to-confirm gate in the viewer; the deletion is performed by atomic rewrite, preserving other sessions, and is itself sealed in Vault A.

### 5. Your Rights Under the EU AI Act

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

The EU AI Act establishes specific rights for users of AI systems. SOSA DevOps's design honours each of the relevant rights for v1.0:

Right to know when AI is in use. Every chat turn in the Software shows the Model name in the response header (for example, "llama3.1:8b") and the persona attribution if a persona was active. The presence of the Synopsis module itself is the disclosure that you are talking to AI; we do not impersonate a human.

Right to human oversight. Every AI suggestion can be discarded, edited, or regenerated. The Software does not act on AI Output without you. There is no auto-execute path in v1.0 that takes an AI Output and uses it to modify a file, send a message, or perform any other action without your explicit confirmation. (When agentic routing is fully wired post-launch, this commitment will be reaffirmed: each step in an agent plan will require your review before the next step runs, unless you specifically configure the agent to run autonomously, in which case you accept that responsibility.)

Right to explanation. This right is partially honoured because the internals of an LLM are opaque even to its authors -- we cannot explain why a Model produced a specific token. What we can explain, and do, is:

- \* the Model used (visible per turn),
- \* the persona prefix applied (visible in persona settings),
- \* the RAG chunks that were retrieved (visible in the Vault B `rag\_retrieval` row, with the source document path attached to each chunk).

For non-RAG turns, the explanation surface is "the Model produced this output from your prompt"; we do not pretend to offer more.

Right to export AI operation history. Per-session export from the Vault B viewer in TXT, PDF, or JSONL format. The branded PDF includes an integrity certificate.

Right to delete. Per-session delete from the Vault B viewer; whole-application removal by uninstalling and deleting the application data directory (the v1.1 in-application "delete everything" command will offer a more convenient surface).

Right to lodge a complaint. EU users may complain to the AI Office once it is fully operational, or to the data protection supervisory authority of their member state for any privacy-related aspect of AI use.

## 6. Model Provenance and Licenses

SOSA DevOps does not bundle, host, or distribute LLM weights. When the Software invokes a Model, it invokes a Model that you have installed locally through Ollama. The legal and provenance relationship for the Model is between you and the Model's author.

For convenience, the in-application catalog shows the Model name, family, parameter count, recommended hardware, and license at a glance. The licenses you should expect to see for the most common Models are:

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

```
* **Llama 3.1 (Meta)** -- Llama 3.1 Community License
* **Llama 3.2 (Meta)** -- Llama 3.2 Community License
* **Qwen 2.5 (Alibaba)** -- Qwen Research License or Tongyi Qianwen License (varies
by parameter size)
* **Mistral, Mixtral (Mistral AI)** -- Apache 2.0 (some variants), Mistral Research
License (others)
* **Phi 3 (Microsoft)** -- MIT License
* **Gemma (Google)** -- Gemma License
* **DeepSeek-R1, DeepSeek-V3 (DeepSeek)** -- MIT License
* **nomic-embed-text, nomic-embed-text-v2-moe (Nomic)** -- Apache 2.0
```

You are responsible for license compliance with the Model you have pulled. Some Model licenses restrict commercial use, restrict use against the Model author's competitors, impose attribution requirements, or limit redistribution. The catalog in the application is descriptive metadata, not a legal authority; the authoritative license text is the one published by the Model's author. Read it before you commit to a Model for a use case that depends on its license terms.

The full reference catalog with our reading of each Model's posture lives at docs/architecture/MODEL\_CATALOG.md. We update it as we add or audit models.

### 7. Risk Classification Under the EU AI Act

The EU AI Act classifies AI systems into risk tiers: prohibited, high-risk, limited-risk (transparency obligations apply), and minimal-risk.

SOSA DevOps's AI features are limited-risk. Specifically:

- \* The Software is a general-purpose creative and developer tool. It is not used for any of the high-risk applications enumerated in Annex III of the AI Act: education access, employment decisions, access to essential public or private services, law enforcement, migration and border control, justice and democratic processes, biometric identification, or critical infrastructure.

- \* The Software is **not** a foundation model. We do not train, fine-tune, or distribute Models. We are a consumer of locally-installed third-party Models. The general-purpose AI obligations on foundation-model providers do not apply to us. They apply, separately, to the authors of the Models you choose to pull.

- \* The Software interacts with you, a natural person, and that triggers the transparency obligation under Article 13. This document is the primary instrument for satisfying that obligation. The in-application surfaces (model name in every chat turn, the Synapsis module's clear AI framing, the access to Vault A and Vault B) are the secondary instruments.

We do not deploy AI in any decision-making capacity that affects your legal rights, your safety, or your access to essential services. If you choose to use AI Output for such purposes, you do so on your own judgment and at your own responsibility, as discussed in §8.

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

### 8. Out-of-Scope AI Uses

The Software is not authorised, validated, or warranted for the following uses, and we discourage you from relying on AI Output for any of them:

- \* medical advice, diagnosis, clinical decision support, or any aspect of patient care;
- \* legal advice, contract drafting for execution, or any aspect of legal practice that would normally require a licensed practitioner;
- \* financial trade decisions, investment advice, or any decision affecting another party's assets;
- \* safety-critical system control or any system whose failure could cause physical harm;
- \* biometric identification or surveillance;
- \* regulated content moderation (for example, broadcast compliance);
- \* decisions affecting an individual's access to essential services, education, employment, or credit.

This list is also given in the Terms of Service §6. It is duplicated here because the AI Disclosure is the document a user reads when they want to understand the AI itself, and "what is this AI not for?" is a question about the AI.

If your use case appears in the list above, the responsibility for that decision is yours, and we recommend professional human review before any AI-influenced decision is acted on.

### 9. External API Providers -- Deferred to v1.1+

v1.0 ships with no external API providers wired. The architecture supports them; the catalog tab shows them as Disabled; no code path produces a network request to any third-party AI service.

When external providers are wired in v1.1+, this document will be revised to disclose, for each provider:

- \* the provider's identity and jurisdiction,
- \* the provider's published privacy policy and AI policy,
- \* the data the Software sends (prompt, RAG context if any, model parameters),
- \* the **Privacy Filter** preflight stage, which inspects and redacts the outbound payload before the request leaves the device. The Privacy Filter is currently a Stage 1 stub; its rule engine and redaction surface ship with the first concrete provider.
- \* the **logging behaviour** for external requests (Vault A seals the event; Vault B records the prompt and response with ``direction`` set to ``user_to_api`` and ``api_to_local``).

Until that document revision lands, the v1.0 invariant is simple: no AI request leaves your device.

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

The first concrete provider on the roadmap is DeepSeek. The application's design treats every external provider as a user-keyed integration: you bring the API key, the Software does not proxy through any Sovereign Systems server, and your billing relationship is with the provider, not with us.

### 10. Contact

- \* AI-specific questions: `ai@sovereignsystems.cc`
- \* Privacy questions: `privacy@sovereignsystems.cc`
- \* Legal questions: `legal@sovereignsystems.cc`
- \* Security disclosure: `security@sovereignsystems.cc`

If you are an EU resident exercising rights under the AI Act and you would like a structured response, indicate that in your email so we can route it appropriately.

Sovereign Systems  
Thailand

## SOSA DevOps

Sovereign Systems - AI Disclosure

---

### Document Integrity Certificate

---

**Document:** AI Disclosure

**Application:** SOSA DevOps v1.0.0

**Publisher:** Sovereign Systems, Thailand

**Effective Date:** 2026-05-21

**Generated:** 2026-05-21

**Source SHA-256:** c996f647be2c9e1a7b5ff55a10cd7d88

**(cont):** 758e35f65a355b15228fe279cee4f951

This certificate records the SHA-256 digest of the markdown source from which this PDF was generated. It is provided for audit and tamper-evidence purposes. Sovereign Systems reserves the right to update these documents; the current version is always available in-application.