



Firm AI Policy Package: Glossary

Plain language definitions of the technology and the package's terms of art.

Written to ISO 24495-2:2025; one term per concept, defined before first use.

Account tiers. The levels a vendor sells. Consumer and free accounts may train on your inputs. Team and business tiers are no-training with a stated retention period. True zero data retention usually requires an enterprise agreement.

Add-in. A vendor's AI program that runs inside another application, usually Word. It signs in to a vendor account and sends the open document to that account. Also sold as a plugin.

Agentic AI. A system that plans and completes multistep tasks with little or no real-time human direction. It can select tools and act, not just answer.

AI Policy Administrator. The person the firm names to keep the Approved Tool List, vet new tools, coordinate training, and review the policy.

API (application programming interface). A direct software connection that sends a request to a model and returns the answer. API channels are where vendors most often sign zero data retention terms.

Approved Tool List. A one-page table at the back of the policy (Appendix A). Each row is one vetted tool: the product, the account and tier, the required settings, the retention terms, the permitted input tier, and the approval date. Personnel may use only listed tools, in the listed configuration, for client work.

ASD-STE100. ASD-STE100 Simplified Technical English, Issue 9 (January 15, 2025). A writing standard from Europe's aerospace industry, built for aircraft maintenance manuals, where a misread sentence costs lives. It caps sentence length, allows one instruction per sentence, requires the active voice, and gives each word one approved meaning. This package applies it to the text inside graphics, checklists, and rules of conduct: the lines a reader must parse correctly on the first pass.

Assembled context. The specific text a harness collects and sends to the model for one request. Only this content leaves the firm; the rest of the working set stays in place.

Chatbox. A vendor's chat website or app. Everything you type, paste, or attach goes to the vendor's cloud.

Conversation store. The vendor's saved record of your chats and uploads. It persists until someone deletes it, and deletion completes on a delay measured in weeks.

Covered model. A frontier model whose vendor keeps a safety window even under zero data retention terms. Anthropic's Fable 5 is the current example.

Data processing addendum (DPA). A short attachment to a vendor's service contract. It states, as enforceable terms, what the vendor may do with your data: process it only on your instructions, keep it confidential, secure it, report breaches, and delete it on request. A privacy page is documentation the vendor can rewrite; the DPA is a signature.

Embedded AI. An AI feature inside software not usually thought of as AI: research platforms, PDF tools, videoconference assistants. An embedded feature is a tool, and it stays off for client work until vetted.

Generative AI. A system that creates new content, such as text, images, code, or analysis, in response to prompts. ChatGPT, Claude, Gemini, and Copilot are examples.

Harness. An agentic environment that works over a folder of files the firm controls. Documents, instructions, logs, and memory stay in that folder; only the assembled context goes to the model.

Inference. The computation that produces a model's answer to a request. It happens wherever the model runs: the vendor's cloud, or firm hardware for a local model.

Input tiers (Tier 1, 2, 3). The policy's three classes of input. Tier 1: public or fully anonymized material, any approved tool. Tier 2: client documents and matter facts, enterprise-configured approved tools only. Tier 3: sealed, protected, or client-restricted material. Stop

and ask the responsible attorney.

Local model. A model that runs on hardware the firm controls. Nothing transits to any vendor.

Memory. A profile of you and your work that a tool consults across sessions; vendors also call it personalization. Cloud memory can carry one client's information into another client's session. In a harness, memory is a readable file in the matter folder.

Model. The AI system that reads a request and produces the answer. One vendor offers many models, with different capabilities and different retention terms.

Placeholder. A fictitious name or label that replaces a client identifier before text goes to a cloud tool: John Doe, Blackacre, [ACCT-1]. Substitution happens before transmission, and the key stays in the matter file.

Privacy Mode. Cursor's setting that routes all model traffic under its zero data retention agreements. A Tool List entry records it as part of the approved configuration.

Safety window. A fixed period, currently 30 days, that a covered model's vendor keeps inputs for trust and safety review, even under zero data retention terms. Flagged content can be held longer. The window follows the model, not the account.

Session log. The saved record of what a tool did in a session. In a harness it is a local file in the matter folder: billing, troubleshooting, and the policy's documentation duty all read from it. On cloud tools, the vendor's conversation store is the only record.

Subprocessor. A company a vendor uses to deliver its service, such as model providers and cloud hosts. Contract terms must bind subprocessors, or the vendor's promises stop at the vendor.

Tenant. The firm's own licensed partition of Microsoft's cloud. A tenant is still a vendor's cloud: Microsoft holds the data, and the credentials that guard it live outside the firm's own systems. Microsoft 365 Copilot runs inside the tenant; treat it as a vendor relationship to vet, not a safe harbor.

Training. A vendor's use of your inputs to improve its models. The policy bars client work wherever training is on.

Upload-first. An architecture in which every document a tool works on migrates to the vendor's cloud before anything happens. The legal platforms are upload-first by their own terms.

Way of working. How the firm touches a model: the chatbox, the add-in, or the harness. The same vendor can appear in all three, with a different data footprint in each.

Working set. The folder of documents, instructions, logs, and memory that a harness works over. It stays on firm storage.

Zero data retention (ZDR). A contract term: the model provider does not store your inputs or outputs and does not train on them. It governs training and storage. It does not govern memory settings, and the covered-model safety window is its one standing exception.