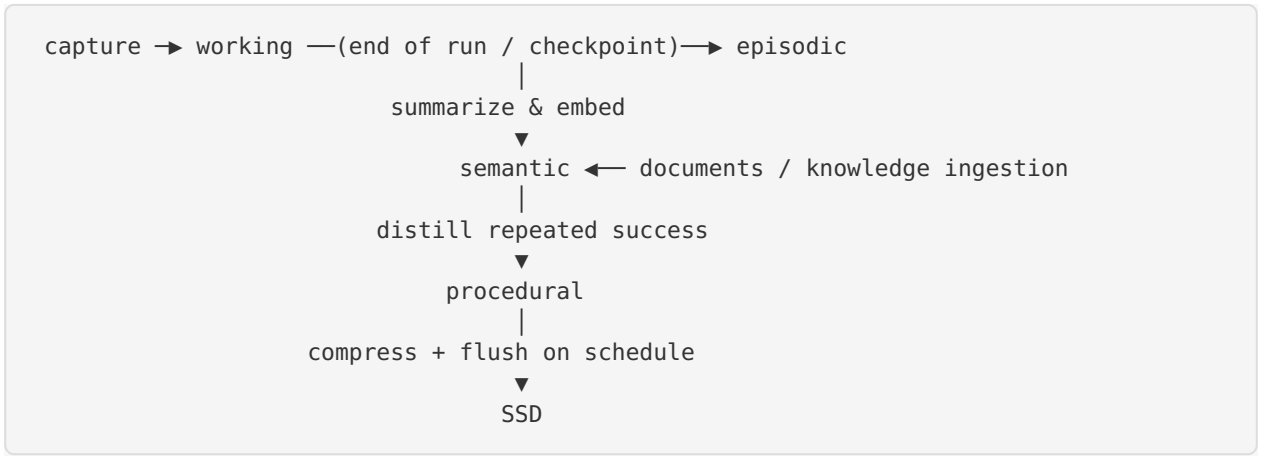
ALPHA Agent Memory Model

This document defines how agents in ALPHA remember. The **Memory Store (SSD)** module visualizes this model; in the
current build all entries are simulated (`lib/mock-data.ts → memoryEntries`).

Memory Tiers

Tier	Purpose	Lifetime	Typical store (target)	Access pattern
Working	Current task context, scratch-pad, tool results	Single run	In-process / Re-dis	Read-write, hot
Episodic	What happened: events, conver-sations, run transcripts	Days → months	Relational DB + object storage	Time-ordered append
Semantic	What is known: facts, docu-ments, embed-dings	Long-lived	Vector DB (pgvector, Pinecone, Weavi-ate)	Similarity search
Procedural	How to do things: learned playbooks, prompts, tool re-cipes	Long-lived, ver-sioned	Relational DB	Lookup by skill/ intent
SSD (persist-ent)	Compressed, durable snapshots of the tiers above	Retention policy	Object storage / NVMe	Flush & restore

Lifecycle



Memory Record Schema (target)

```
{
  "id": "mem_01J...",
  "agentId": "orchestrator-prime",
  "type": "episodic | semantic | working | procedural | ssd",
  "key": "run:4521:summary",
  "value": "…",
  "embedding": [0.012, -0.44, "…"],
  "sizeBytes": 2048,
  "createdAt": "2026-09-27T12:00:00Z",
  "lastAccessedAt": "2026-09-27T12:05:00Z",
  "ttlSeconds": null,
  "sensitivity": "public | internal | confidential | restricted",
  "provenance": { "source": "tool:web-search", "traceId": "…" }
}
```

Rules

1. **Least privilege** — an agent reads only its own memory plus explicitly shared namespaces.
2. **Provenance required** — every write records its source and trace ID so poisoned memories can be traced and purged.
3. **Sensitivity labels** — `restricted` data (credentials, payment data, PII) is never embedded and never stored in working memory longer than one step.
4. **Untrusted content stays untrusted** — text retrieved from the web or tools is stored as data, never promoted to procedural instructions without review.
5. **Garbage collection** — stale working/episodic entries are expired per TTL; SSD snapshots follow the retention policy.
6. **Right to erasure** — bulk delete by agent, namespace, or subject must be supported.

Operations exposed in the UI

Browse · semantic search (top-K with similarity) · per-agent timeline · knowledge-graph view · SSD per-sistence
metrics (compression ratio, retrieval latency) · bulk clear / export / import / GC.