Memoir.ai — Printable Technical Specification

Version: 1.0

Status: Printable Technical Reference

Owner: Platform Architecture Team

Last Updated: YYYY-MM-DD

1. Purpose

This document provides a printable technical specification for Memoir.ai, summarizing system architecture, data flows, processing pipelines, storage models, and operational constraints required for engineering, auditing, and enterprise review.

2. System Overview

Memoir.ai consolidates fragmented digital archives into a unified encrypted timeline. The system combines ingestion pipelines, background processing, AI-assisted narrative generation, and hybrid search while maintaining strict local-first data ownership.

3. Architecture Summary

The platform operates as a desktop system composed of an Electron shell, React renderer, background worker processes, encrypted vault storage, ingestion pipelines, job queues, AI narrative generation, and hybrid search services.

4. Execution Model

A multi-process model isolates heavy computation from user interaction. The main process controls lifecycle and filesystem access, the renderer hosts the interface, and workers execute ingestion, indexing, and AI tasks.

5. Storage Model

User data resides within an encrypted SQLCipher vault containing events, narratives, and attachments. Encryption keys exist only in memory while unlocked. Configuration data is stored separately without sensitive information.

6. Ingestion Pipeline

Archives are parsed, validated, normalized, deduplicated, and stored as canonical event records. Background jobs enable resumable imports and checkpoint recovery.

7. AI Narrative Pipeline

Selected events are transformed into citation-backed narratives through evidence sampling, prompt construction, local inference, verification checks, and versioned persistence.

8. Search & Indexing

Hybrid retrieval combines lexical full-text search with semantic vector search, providing fast timeline exploration while keeping indices encrypted inside the vault.

9. Background Job System

All heavy operations run through a job queue supporting priority scheduling, retries, checkpointing, and crash recovery.

10. Security & Privacy Controls

Security measures include encrypted storage, process isolation, strict IPC validation, sanitized logging, and prohibition of remote storage for personal vault content.

11. Performance Targets

The system aims for responsive UI interaction, sub-second search results, efficient imports, and bounded memory usage through throttled background execution.

12. Data Portability

Users can export complete archives using open formats, structured JSON schemas, and media bundles ensuring long-term independence from vendor tooling.

13. Reliability & Recovery

Resumable ingestion, integrity checks, backup restoration, and worker crash recovery ensure data remains accessible under failure conditions.

14. Future Expansion

Planned enhancements include device synchronization, collaborative vaults, improved semantic reasoning, and advanced indexing strategies while preserving compatibility.

15. Conclusion

Memoir.ai provides a privacy-first technical foundation for personal archive reconstruction and AI-assisted narrative intelligence while maintaining user ownership and portability.