

Memoir.ai — Formal Operations Manual

AI Operations & Platform Governance

Document Control

Document Title: Memoir.ai Formal Operations Manual

Version: 1.0

Status: Operational Draft

Owner: Platform Operations

Last Updated: YYYY-MM-DD

Purpose

This manual defines operational, governance, safety, security, and execution standards governing the Memoir.ai AI subsystem and platform services. It serves as the authoritative reference for engineers, operators, QA, and support teams responsible for maintaining system stability, privacy guarantees, and operational continuity.

Scope

This manual covers:

- AI subsystem execution and safeguards
- Narrative generation pipeline operations
- Evaluation and hallucination controls
- User control safeguards
- Security and privacy enforcement
- Billing and entitlement enforcement
- Deployment and CI/CD operations
- Logging, monitoring, and recovery procedures

User-facing product guides are excluded unless required for operational impact.

Audience

- Platform engineers
- DevOps operators
- Security auditors
- QA teams
- Technical support
- Product leadership

System Overview

Memoir.ai operates as a local-first platform with optional cloud synchronization for identity and billing metadata. AI operations execute primarily on-device, ensuring personal data remains private and encrypted.

Core operational principles:

- Local execution by default
- Citation-backed narrative generation
- Strict privacy preservation
- Immutable versioning of narratives
- User authority over AI outputs

AI Operational Flow

Snapshot Generation Pipeline

1. User selects evidence or time slice.

2. Extraction identifies entities and anchors.
3. Local model performs inference.
4. Hallucination guards verify claims.
5. Citations are mapped to source events.
6. Output is sanitized and stored.
7. Narrative versions are archived.

Version Management

- Every regeneration creates an immutable version.
- Manual user edits are preserved.
- Only five recent versions retained unless pinned.

Citation Enforcement

- Citations inserted at sentence level.
- Media citations flagged appropriately.
- Conflicting evidence generates conflict tags requiring resolution.

AI Governance & Safety

Hallucination Guards

Operations include:

- Entailment verification between claims and evidence.
- Entity matching against metadata.
- Tone neutrality enforcement.

Failure results in flagged sentences or regeneration prompts.

Quality Evaluation

Snapshots are evaluated using:

- Factual accuracy metrics
- Narrative coherence scoring
- Citation density thresholds

Snapshots scoring below verification threshold are marked unverified.

Sensitive Content Handling

AI systems must:

- Avoid medical, psychological, or legal diagnoses.
- Avoid speculation of malicious intent.
- Avoid financial advisory content.
- Redact sensitive identifiers in public summaries.

User Authority Controls

Users may:

- Override AI-generated text.
- Regenerate sections or entire narratives.
- Disable narrativization entirely.

Security & Privacy Operations

Access Control

- Vault access restricted via OS-level permissions.

- Strong passphrase enforcement.
- Auto-lock configurable.

Encryption Strategy

- SQLCipher AES-256 encryption for vault storage.
- Media encrypted individually.
- Keys never stored on disk.
- Sensitive memory cleared after use.

Telemetry Policy

- Zero telemetry by default.
- Optional anonymized diagnostics only.
- No personal content transmitted.

Data Lifecycle Operations

Retention Policy

- Data retained indefinitely unless user deletes.
- Optional auto-clean policies configurable.

Secure Deletion

- Event records removed from database.
- Media files purged if orphaned.
- Vault wipe removes database, attachments, and caches.

Export Guarantees

- Data export always available.
- Open formats only.
- Exports function offline.

Billing & Entitlements Operations

Subscription State Handling

States include:

- Active
- Trialing
- Past Due
- Canceled
- Expired

Local caches preserve entitlements during offline use.

Usage Metering

Metered resources:

- AI token generation
- Source count
- Storage consumption

Exceeding limits disables restricted features until reset.

Stripe & Auth Integration

- Subscription updates via webhook processing.

- Entitlements verified before costly operations.

Operational Infrastructure

CI/CD Pipeline

Release pipeline includes:

- Linting and testing
- Security scanning
- Build packaging
- Smoke tests
- Artifact distribution

Release Gates

Production releases require:

- Full test pass
- Security validation
- Performance thresholds met
- Product approval

Logging & Observability

Logs capture:

- Authentication events
- Import and export actions
- System lifecycle events

Logs must not contain private user content.

Monitoring & Alerts

System monitors:

- Disk availability
- Database performance
- Worker memory consumption

Alerts displayed via UI or system notifications.

Incident Response

Vault Corruption Handling

- Attempt automatic repair.
- Restore from backup if necessary.

Local Breach Handling

Users instructed to:

- Isolate device.
- Export critical data.
- Wipe compromised vault.

Technical Support

Support never requests passphrases or private data.

Rollback Procedures

- Pause auto-updates.

- Revert distribution pointers.
- Provide downgrade paths when possible.

Operational Responsibilities

Engineering Teams

- Maintain pipeline performance.
- Enforce schema and security rules.

Security Teams

- Audit encryption and access controls.
- Review threat models.

QA Teams

- Validate state handling and privacy isolation.

Conclusion

This manual defines operational standards ensuring Memoir.ai maintains privacy, reliability, and narrative integrity while preserving full user ownership over personal data.