Memoir.ai — Security & Compliance Handbook

Platform Security, Privacy, and Regulatory Alignment

Document Version: 1.0

Status: Operational Reference

Owner: Security & Compliance

Last Updated: YYYY-MM-DD

---

1. Purpose

This handbook defines the security principles, operational safeguards, and regulatory alignment practices governing Memoir.ai. It serves as the primary reference for engineers, operators, auditors, and compliance reviewers responsible for ensuring user data remains private, protected, and under user control.

---

2. Scope

This handbook covers:

• Data protection mechanisms

• Access control and authentication safeguards

• Encryption standards

• Privacy enforcement

• Compliance alignment

• Audit logging

• Incident response

• Secure data lifecycle management

• Billing and entitlement data safeguards

This handbook applies to all components interacting with Memoir.ai vault or metadata systems.

---

3. Security Philosophy

Memoir.ai is built on the following principles:

• Local-first data ownership

• Encryption by default

• Zero data exfiltration without consent

• User-controlled data lifecycle

• Minimal data exposure

• Transparent and auditable operations

The platform must never assume ownership of user content.

---

4. Threat Model Overview

Primary threat vectors include:

• Unauthorized local access

• Theft of physical storage

• Malicious import files

• Malware memory scraping

• Credential compromise

Mitigation strategies include encryption at rest, vault locking, sandbox parsing, and memory sanitization.

Threats outside application control, such as full kernel compromise, remain out of scope.

---

5. Access Control Standards

Physical Access:

• Vault access restricted by operating system permissions.

• Direct file access must require authenticated OS user.

Logical Access:

• Vault unlock requires strong passphrase.

• Auto-lock after inactivity.

• Renderer processes isolated from file system access.

Remote Access:

• No built-in remote access features.

• Support assistance must occur through user-controlled screen sharing only.

---

6. Encryption Strategy

Database Encryption:

• SQLCipher encryption using AES-256.

• Strong key derivation via PBKDF2 or Argon2id.

Key Handling:

• Passphrases never stored.

• Keys generated at runtime only.

• Sensitive memory buffers cleared immediately after use.

Media Encryption:

• Attachments encrypted individually.

• Decryption keys stored only within encrypted vault.

In-Memory Protection:

• Key material marked non-swappable where possible.

• Buffers sanitized after operations.

---

7. Privacy Enforcement

Telemetry:

• Disabled by default.

• Opt-in diagnostics limited to anonymized performance data.

• Personal content never transmitted.

Data Transmission:

• Narrative generation occurs locally.

• Cloud sync transfers metadata only when enabled.

AI Safety:

• AI must avoid diagnosing or speculating about individuals.

• Sensitive personal data must be redacted in public summaries.

---

8. Data Lifecycle Management

Retention:

• Data stored until user deletes it.

• Optional cleanup policies configurable.

Deletion:

• Event deletion removes database records.

• Media removed when orphaned.

• Vault wipe deletes databases, attachments, and caches.

Export:

• Full export always available.

• Uses open, portable formats.

• Offline export supported.

---

9. Audit Logging

Logged events include:

• Vault unlock attempts

• Data import/export actions

• Configuration changes

• System update events

Audit logs must:

• Exclude personal content

• Avoid participant names or message text

• Use hashes instead of identifiers when needed

Logs automatically rotate after retention thresholds.

---

10. Compliance Alignment

GDPR & CCPA Alignment:

• User acts as data controller.

• Application acts as processing tool.

• Data export supports access rights.

• Vault deletion fulfills erasure requests.

• Portable formats satisfy portability rights.

Zero-Knowledge Compliance:

• Vendor cannot access user data.

• External legal requests cannot expose content stored locally.

---

11. Billing & Metadata Safeguards

Billing data protections include:

• Subscription data separated from vault content.

• Payment operations handled via Stripe.

• Entitlements cached locally for offline operation.

Metadata synchronization excludes private message content.

---

12. Incident Response

Vault Corruption:

1. Attempt repair.

2. Restore backup if needed.

Local Breach Response:

1. Disconnect system.

2. Export critical data.

3. Perform vault wipe.

Security Incident Handling:

• Preserve logs.

• Patch vulnerabilities.

• Issue remediation guidance.

Support teams must never request passphrases.

---

13. Secure Development Practices

Engineering teams must:

• Validate all IPC messages.

• Avoid logging sensitive data.

• Keep dependencies patched.

• Apply schema validation to inputs.

• Enforce least privilege policies.

Security reviews required before major releases.

---

14. Operational Security Monitoring

System monitors:

• Disk exhaustion risks

• Database latency spikes

• Worker memory limits

• Background job failures

Alerts presented locally without leaking private data.

---

15. Backup & Recovery Guidance

Recommended safeguards:

• Automatic backups enabled.

• Users encouraged to export periodically.

• Backups stored on external or encrypted media.

---

16. Security Best Practices Summary

• Use strong vault passphrases.

• Keep operating systems updated.

• Maintain encrypted backups.

• Verify imports from trusted sources.

• Review generated narratives for correctness.

---

17. Conclusion

This handbook establishes operational security and compliance foundations for Memoir.ai. By enforcing encryption, privacy preservation, and strict data ownership, Memoir.ai maintains a secure and compliant environment for personal history preservation.