Memoir.ai — Enterprise Deployment Guide (Expanded)

Document Version: 1.1

Status: Enterprise Operational Reference

Owner: Platform Architecture & Operations

Last Updated: YYYY-MM-DD

Purpose & Audience

This guide enables enterprise IT teams to deploy Memoir.ai safely and consistently across managed environments.

The intended audience includes infrastructure administrators, endpoint management teams, and deployment engineers.

Deployment Models

Supported models include managed workstation deployment, controlled lab environments, and secure research or compliance workstations.

Deployments may occur via MDM tooling, software distribution systems, or controlled installation workflows.

Infrastructure Preparation

Confirm endpoint storage capacity and encryption compliance.

Ensure endpoint OS patch levels meet organizational standards.

Validate secure storage paths for vault data.

Installation Procedures

Distribute installer via enterprise deployment tooling.

Verify application installation integrity using checksums.

Confirm application launch and vault initialization success.

Vault Storage Governance

Define approved vault storage directories.

Prevent vault storage on unsecured removable drives.

Enforce enterprise backup and encryption requirements.

Deployment Validation Steps

Verify vault creation and unlock flows.

Confirm ingestion workflows execute successfully.

Confirm entitlement checks succeed.

Operational Risks & Mitigation

Incorrect storage policies may expose data risk; enforce endpoint policies.

Import failures must be mitigated via resumable ingestion and worker monitoring.

Maintenance & Lifecycle

Plan quarterly validation of deployment compliance.

Maintain installer version control and rollback capability.

Revision History

Version 1.1 expands deployment procedures and operational governance.