

DECISIONFLOW

Technical Shutdown and Service Decommissioning Runbook

Sequencing read-only transition, AI cutoff, data disposition, infrastructure removal, and final verification

RETIRE PHASE | Version 1.0 | Illustrative controlled retirement and knowledge-preservation program

EVIDENCE & PUBLISHING INTEGRITY

This public portfolio edition distinguishes actual evidence, assumed continuity steps, simulated case-study outcomes, targets, and recommendations. Simulated customers, commercial results, benchmarks, incidents, quotations, and later-lifecycle outcomes are illustrative and must not be interpreted as results from a live commercial product. Evidence labels are retained throughout the package to support transparent and responsible interpretation.

Document Control

Control	Definition
Document code	RET-04
Version / status	2.0 — Final Public Portfolio Edition — Simulated Retirement Scenario
Baseline / author	14 July 2026 - Min Thu Kyaw
Scenario horizon	Illustrative 24-month post-scale operating period followed by a 180-day retirement program.
Lifecycle continuity	Actual MVP -> assumed productionization -> simulated Launch -> Qualify -> Deliver -> Controlled Scale -> Retire.
Retirement decision	Retire the standalone service through a controlled transition while preserving reusable product, AI, and technical assets.
Scope boundary	No new collaboration, integration, richer-ingestion, multilingual, SSO, or enterprise-platform build is assumed.
Evidence rule	Actual, assumed, simulated, target, recommendation, and verified-shutdown statements are separated.

Actual Project Artifacts

Artifact	Reference
Low-Fidelity Prototype	View prototype
High-Fidelity Prototype	View prototype
MVP Frontend Repository	Open repository
MVP Backend Repository	Open repository

Contents

01	Runbook purpose and authority
02	System and dependency inventory
03	Pre-shutdown gates
04	Ordered shutdown sequence
05	Rollback and incident controls
06	Repository, DNS and monitoring closure
07	Final technical verification

Runbook Purpose and Authority

Execution rule - No resource is deleted because a calendar date arrives. Each destructive step requires its prerequisite gate, accountable approver, evidence capture, and rollback assessment.

System and Dependency Inventory

Component	Illustrative implementation	Retirement action
Frontend	Next.js web application and static assets.	Switch to notice/read-only experience, then archive and remove hosting.
Backend API	FastAPI services and ownership controls.	Disable writes and AI generation, preserve export/retrieval endpoints temporarily, then shut down.
Database	PostgreSQL with users, decisions, criteria, transcripts, recommendations, history.	Freeze schema, complete exports, delete/retain by policy, archive evidence, remove cluster.
AI provider	OpenRouter-compatible provider and model configuration.	Stop requests, revoke keys, close processor obligations.
Object/export storage	Temporary downloadable archives and operational files.	Expire exports and delete buckets after verification.
Jobs and schedulers	Evaluation, analytics, lifecycle, cleanup, monitoring tasks.	Disable in controlled order; retain only retirement jobs until completion.
Auth and secrets	JWT/session, encryption keys, environment secrets.	Revoke, rotate, archive evidence, remove from secret manager.
Observability	Logs, metrics, traces, alerts, uptime checks.	Retain transition monitoring, then archive approved evidence and remove alerts.
DNS and certificates	Public domains, API endpoints, TLS certificates.	Redirect to closure notice, then retire or retain domain defensively.

Pre-Shutdown Gates

Gate	Pass criterion	Approver
Customer readiness	Every active account contacted; export/deletion disposition tracked.	Customer Success
Data readiness	Authoritative inventory, retention rules, legal holds, and deletion jobs validated.	Privacy / Legal
Billing readiness	Subscriptions, renewal rules, credits, and payment mandates reconciled.	Finance
Technical readiness	Read-only, export, backup, rollback, and shutdown tests pass in staging.	Engineering / Platform
Security readiness	Secrets, access, provider, and archive controls approved.	Security
Support readiness	Runbook, staffing, escalation, status page, and customer messages active.	Support Lead
Executive go/no-go	No critical issue or unresolved contractual/data obligation.	Executive Sponsor

Ordered Shutdown Sequence

- Freeze feature releases and non-retirement schema changes.
- Stop new subscriptions and renewal creation.
- Enable persistent retirement notice and export-status messaging.
- Disable new AI extraction and recommendation generation.
- Move application into read-only mode while retaining authenticated export and retrieval.
- Complete customer exports, deletion elections, legal-hold segregation, and billing closure.
- Drain asynchronous queues and stop lifecycle, evaluation, and notification jobs.
- Take final evidence snapshot and verify rollback copy within the approved window.
- Disable public API writes, then all customer API access after the final retrieval window.
- Delete eligible active data and temporary exports; validate derivative stores.
- Revoke provider, application, database, storage, CI/CD, and monitoring credentials.
- Remove compute, database, queues, storage, monitoring, and network resources in dependency order.
- Update DNS to final closure notice or defensive holding page; manage certificate expiry.
- Archive repositories, architecture, runbooks, evidence, and knowledge-transfer materials.
- Complete final inventory at zero active production resources and close the incident watch period.

Shutdown dependency checkpoints

Checkpoint	Must be true before proceeding
Disable AI generation	Customer notice is active; support and export remain available.
Read-only mode	Write-block tests pass; retrieval and export are reliable.
API shutdown	All customer dispositions are complete or approved exceptions exist.
Database deletion	Evidence snapshot, legal holds, billing/legal retention, and deletion jobs are approved.
Secret revocation	No remaining transition workload depends on the credential.
Infrastructure deletion	Rollback window is closed and all evidence is archived.

Rollback and Incident Controls

Failure mode	Immediate response	Rollback / recovery
Export mismatch	Pause affected exports and shutdown dependency.	Restore read-only service from verified rollback copy; reconcile counts.
Unexpected authorization failure	Disable public transition action and invoke security incident process.	Revert to last approved release and rotate affected secrets.
Billing continues	Suspend payment integration and notify affected accounts.	Issue credits/refunds and reconcile provider state.
Deletion exceeds approved scope	Stop deletion workers and preserve logs.	Restore only from approved backup under privacy/legal direction; notify according to incident policy.
Provider credential still active	Revoke immediately and inspect usage.	No rollback; complete exposure assessment and evidence.
Critical customer issue near deadline	Extend affected customer access without extending all production writes.	Use controlled exception environment or assisted export.

Repository, DNS and Monitoring Closure

- Tag the final production release and shutdown commit.
- Scan repository history, CI variables, documentation, and artifacts for secrets before archival.
- Set repositories read-only, preserve licences and attribution, and document future owner.
- Remove deployment keys, GitHub Actions secrets, webhooks, tokens, and automation credentials.
- Redirect public domains to a closure notice for the approved period; retain domain defensively where brand or phishing risk exists.
- Replace availability alerts with retirement verification checks, then close monitoring accounts after the observation period.

Final Technical Verification

Verification	Simulated result	Evidence
Production resources closed	43/43	Cloud inventory and billing report.
Public write paths	0 active	API and browser smoke tests.
AI generation paths	0 active	Feature-flag, provider-usage, and credential evidence.
Secrets and service accounts	Revoked or deleted	Secret-manager and identity inventory.
DNS / certificates	Closure state verified	DNS records and certificate inventory.
Critical shutdown incidents	0	Incident register and final watch report.
Repositories	Archived read-only	Repository settings and security-scan evidence.

Evidence discipline: replace all simulated retirement values with observed, reproducible records before presenting them as actual product performance or compliance evidence.