

INTAKE · CLAUSE RAG · HITL · LEGAL OPS

AI Contract Intelligence & Legal Operations Platform

Dockerized AICL platform for multi-channel intake/OCR, clause RAG, deterministic policy + risk, MCP agents with HITL, obligations/renewals, compare/redline, CLM stubs, and closeout gates — for teams that need governed contract intelligence, not ChatGPT-over-PDF.

M0–M10
MILESTONES CLOSED

PASS
PHASE 1 / MVP / 3

2.1.0
API VERSION

all_pass
M10_GATE

Built by **Abdul Basit** · AI Automation Engineer

BUSINESS IMPACT

Faster review · safer AI · audit-ready legal ops

Intake→RAG→Policy→HITL→Closeout · unauthorized 0 · approval 100% · silent 0

OVERVIEW

Email, upload, and API feed FastAPI OCR/classify into Postgres, MinIO, and Qdrant. Clause RAG is ACL-filtered; policy is deterministic; risk findings are labeled. Agents use MCP allowlists; renewals advise only; redlines create new versions. n8n thin HTTP wraps P0 paths with DLQ. Live prod cutover is formally waived for sandbox acceptance.

- TYPEContract intelligence + legal ops platform (not a single n8n flow)
- ROLEAI Automation Engineer / Legal Ops AI Engineer
- DELIVERYAPI 2.1.0 · Milestone M10 · Closeout 2026-09-12 · Milestones doc v2.1
- STACKFastAPI · n8n · Postgres · Redis · Qdrant · MinIO · OCR/LLM router · CLM stubs
- BUYERSLegal ops / commercial teams needing HITL contract AI with hard gates

THE PROBLEM

- Manual lag — clause hunt
- Renewal misses — notice windows
- Ungoverned AI — invented findings
- Silent edits — binary rewrite
- ACL leaks — search/RAG
- No closeout — hard to prove gates

THE SOLUTION

- FastAPI AICL — agents, HITL, audit
- Thin n8n — intake / renewal wraps
- Clause RAG — evidence spans
- Policy binds AI — labeled risk
- Immutable — redline → new version
- Hard gates — 0 / 100% / 0

WHO IT SERVES

- Legal ops needing **governed contract AI**
- Contract managers needing renewal advise
- Works without live CLM credentials
- Lead demo: **intake** → **HITL** → **m10_gate**
- Secondary: compare / redline / ACL deny

CAPABILITY SURFACES

SURFACE	FOCUS	SURFACE	FOCUS
Intake / OCR	Multi-channel · confidence	Clause RAG	ACL · citations
Policy / HITL	Deterministic · approvals	Obligations	Tasks · renewals advise
P1 / P2	Compare · CLM stubs · learning	Security	ACL · kill switch · DLQ

Demo lead: OpenAPI → demo_6_1 → policy/HITL → kill-switch → m10_gate . **Secondary:** ACL deny · redline new version · renewal advise-only. **Closeout:** POST /m10/fixtures/m10_gate **all_pass**.

Architecture rule: FastAPI owns AI / AuthZ / HITL / policy / ACL · n8n stays thin · CLM optional SoR · no unsupervised legal conclusions · env-only secrets.

ARCHITECTURE & CAPABILITIES

Architecture, journeys, legal safety

Principle: FastAPI owns intake, RAG, policy, agents, HITL, and audit; **n8n owns thin side effects** — CLM/e-sign remain optional systems of record.

Channels (email / upload / API)
→ n8n intake + review + renewal + error path → PostgreSQL + MinIO + Qdrant
→ FastAPI: OCR · clauses/RAG · policy/risk · MCP · HITL · obligations
→ Compare/redline · connectors/CLM stubs · closeout · Redis kill-switch

COMPONENT	ROLE
Host API :18001	Compose-mapped FastAPI 2.1.0 with OpenAPI
FastAPI	Auth (X-API-Key + X-Role), policy, ACL, audit
MCP / kill switch	Per-agent allowlists; blocks write/notify tools
HITL	Approve before sensitive writes / renew decide
Phase 3	Compare/eval, connectors/CLM/K8s/learning, docs/KT

INTELLIGENCE

- OCR + classify + metadata spans
- Clause RAG with ACL filter
- Deterministic policy engine
- Risk labeled policy vs AI
- Eval scorecards + cost meter

INTEGRATIONS

Drive / CRM	Fixtures
CLM / e-sign	Webhook stubs
Tasks / notify	Adapters
K8s guide	Docs
Live vendors	Waived

SAFETY & OPS

- No unsupervised legal conclusions
- Immutable originals / new versions
- Renewals advise-only
- ACL deny proven
- Silent completes = 0

LEAD DEMO PATH

- Health 2.1.0 + OpenAPI
- \$6.1 intake → policy/risk
- HITL approval stage
- Kill switch blocks writes
- POST /m10/fixtures/m10_gate

SECURITY PROOF POINTS

No API key → **401** · MCP overreach denied · ACL deny audited · unauthorized / silent completes: **0** · approval: **100%**.

Reliability, M0–M10, Phase gates, closeout

RELIABILITY AND LEGAL SAFETY

AREA	WHAT SHIPPED
Auth	X-API-Key + X-RoLe
MCP	Per-agent allowlists · audited denies
HITL	Approve before sensitive writes
Policy	Deterministic + labeled risk
Redline	New version only · originals immutable
Audit	Export + closeout snapshot

PHASE GATES + CLOSEOUT

- Phase 1 (M4) — intake/RAG; policy/MCP; injection → 0 - MVP (M7) — §6.1–§6.3; HITL; unauthorized → 0; silent → 0 - Phase 3 (M10) — P1/P2; docs+KT; sandbox Met	
m10_gate	all_pass=true
API version	2.1.0
Closeout date	2026-09-12
Evidence chain	docs/m4 → m7 → m8 → m9 → m10

MILESTONES M0–M10 (ALL COMPLETE)

ID	THEME	WHAT UNLOCKED
M0	Kickoff & architecture	Stack, HITL matrix, legal non-goals
M1–M2	Skeleton → intake	Compose, RBAC, OCR/classify
M3–M4	Clauses → Phase 1	RAG ACL, policy/risk, MCP, Phase 1 Met
M5–M6	Obligations → n8n	Renewals, approvals, §6.1–§6.3
M7	Exceptions / MVP	Dashboard, /mvp/evaluate Met
M8–M9	P1 → P2 polish	Compare/redline/eval, connectors/CLM/K8s
M10	Docs / UAT / KT	Closeout pack, Phase 3 Met, API 2.1.0

INTAKE / RAG

Multi-channel → OCR/classify → clause embeddings with ACL-filtered search and evidence spans.

AGENTS + HITL

- MCP tool allowlists
- Policy vs AI labels
- Approval compliance 100%

OPS + RECOVERY

- Exceptions + playbooks
- Backup/restore smoke markers
- Cutover checklist + KT

Concrete reliability: no-key → 401 · MCP overreach denied · ACL deny · mid-fail → DLQ · unauthorized / silent at UAT: 0 · approval: 100%.

Delivery truth: M0–M10 complete · Phase 1/MVP/3 Met · m10_gate all_pass · API 2.1.0 · cite live /health on :18001.

OUTCOMES · TECH · DEPTH

Stack, UAT, journeys, n8n, residual risks

TECH STACK + REPRODUCE

FastAPI · n8n · Postgres · Redis · Qdrant · MinIO · OCR/LLM router · CLM stubs · Compose AICL

`docker compose up -d --build · POST /m10/fixtures/m10_gate on :18001`

Surfaces: /health · /docs · n8n · Auth: X-API-Key + X-Ro1e

SCOPE HONESTY

- Sandbox-first connectors; live cutover waived
- Sandbox-first connectors without live OAuth
- Waivers: live cutover, live UAT staffing, wet-ink
- Not a CLM replacement — full AICL M0–M10

M10 CLOSEOUT EVIDENCE INDEX

DOC	PURPOSE
UAT.md / ACCEPTANCE.md	Persona paths Met · PRD Complete/Waived · gates
CUTOVER.md / RUNBOOK.md / KT.md	Deploy checklist · day-2 ops · KT notes
ARCHITECTURE_v1.md	Baseline topology
m10_gate / SMOKE.md	Docs · UAT · compliance · acceptance aggregator

OPS

Exceptions	Playbooks
Cost	Metering
Approvals	HITL queues

P1 / P2

Compare / redline	M8
Eval / graph	M8
CLM / learning	M9
K8s guide	Docs

N8N CATALOG

- intake / review / policy
- renewal / obligation
- global error / DLQ

N8N (THIN CALLERS)

Intake · review · policy/risk · renewal · obligation · global error — env API key only

RESIDUAL RISKS (HONEST)

Live Drive/CRM/CLM sandboxes · prod TLS/secret rotation · OCR/LLM quality · wet-ink acceptance — tracked as M10 waivers; **none reopen Phase gates.**

SAMPLE JOURNEYS + GATES

\$6.1 New contract	\$6.2 Renewal advise	\$6.3 Obligation task	HITL Approval 100%
ACL Deny leak 0	Redline New version	Closeout m10_gate	401 No key

PORTFOLIO ONE-LINER

AICL — Dockerized FastAPI + n8n contract intelligence platform: intake/OCR, clause RAG, policy/risk, MCP agents with HITL, obligations/renewals, compare/redline, CLM stubs — M0–M10 complete at API 2.1.0 with unauthorized=0, approval=100%, silent=0.

SYSTEM VISUALS

Architecture & before / after

