PalmerAI - Audit-first AI Governance Gateway

PILOT-READY - EVIDENCE-FIRST - HUMAN-IN-THE-LOOP

One-pager v1 (pilot posture)
Generated: 2026-01-15

WHAT IT IS

A secure gateway designed to enforce policy, approval gates, and audit evidence for AI-driven actions before execution.

DESIGNED FOR

- Security / Compliance / IT stakeholders
- Teams scaling automation with controlled risk
- Procurement-friendly pilots (tight scope, clear outputs)

DEPLOYMENT MODEL

- Cloudflare Workers runtime (edge)
- Auth + policy evaluation in the request path
- Operator console and audit reports (ops/admin)

Details are verified from repo config in the Security Review Pack.

HOW IT WORKS (5 STEPS)

- Send request to Gateway
- Policy evaluation + risk classification
- If triggered - approval required
- Execute / block
- Write audit evidence (metadata)

WHAT WE LOG (EVIDENCE-FIRST)

- Request ID
- Decision: allow / block / approval required
- Policy reference
- Timestamp (UTC)
- Risk level and triggers

Default posture avoids raw prompt storage in audit records unless pilot scope requires it.

PILOT (SINGLE USE CASE - 30 DAYS)

- One primary use case (scope-disciplined)
- Defined risk triggers + approval gates
- An audit report you can share with security / compliance stakeholders
- Clear go / no-go decision and rollout options

SECURITY POSTURE (PILOT-READY)

- Secrets via Cloudflare secrets
- Admin endpoints protected by Bearer tokens
- Rate limits / abuse controls in policy
- Retention is policy-configurable

PROCUREMENT-FRIENDLY NOTES

- No cookies / no tracking on the public website by default
- Evidence-first audit summaries (request ID + policy reference)
- Scope-disciplined pilot (one use case)
- Clear go / no-go success criteria
- Built for security / compliance stakeholders
- Minimal integrations in v1 to keep risk low
- Security and data-handling review pack (pilot-ready) available on request

Contact: contact@palmerai.eu.com
Subject suggestion: `"PalmerAI Pilot - 30 days"`