Third-Party & Vendor Risk Management Policy

Mindshine Technologies Inc. · Document 12 · Version 1.1 · August 12, 2026 · Status: **Operating · one DPA in progress**

The register — actual vendors, actual data flows

A maintained **vendor & subprocessor register** is verified against real data flows (not self-declared usage). Current material vendors:

Vendor	Service	Data that flows there	Posture
AWS	EKS, EC2, EBS, S3, ECR (us-east-1)	All platform data	SOC 1/2/3, ISO 27001 · AWS DPA (GDPR SCCs)
Anthropic	Claude API (assistants, mapping suggestions, enrichment)	Recipe metadata, prompts, excludable sampled rows	SOC 2 Type II · **DPA countersignature in progress**
Atlassian (Bitbucket)	Git hosting + CI	Source code; scoped CI credentials	SOC 2, ISO 27001 · DPA
Google	Workspace identity (staff SSO)	Staff identity claims only — no customer data	SOC 1/2/3, ISO 27001
npm / Docker Hub	Package & base-image supply	None (inbound only)	Mitigated by lockfiles + CI audit gate

The binding rule

A vendor that will receive customer data requires a DPA before integration, and the register is updated in the same change. The one in-flight exception is disclosed rather than hidden: the **Anthropic DPA is in countersignature**; until it closes, projects flagged as containing regulated data keep LLM row-sampling disabled (a per-project switch enforced in the product).

Due diligence & monitoring

Material providers are assessed on service criticality, data access, and compliance evidence (SOC reports, ISO certificates). The register is reviewed with the risk register; a **critical-vendor security review** (2026) is on file. The annual review re-verifies that documented flows still match actual flows.

Termination

When a relationship ends, access and data-sharing are removed (credential revocation is structural — scoped keys, revocable per-app credentials) and the register updated.

Owner: CTO. **Review:** annually and on any new vendor. **Contact:** security@mindshine.com.