

Vendor management policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	Every outside service that stores, processes or receives Final Frame data, or that the build depends on
Review	27 October 2027
MPA CSBP	OR-3.4, PS-3.3, TS-1.11, TS-2.12, TS-7.0 (5.3.2: TS-7.4)

Approved by Robin Ashford, Founder, 27 October 2026

Tiers

Tier	Meaning	What we need before use, and each year
1	Receives customer content (media, documents, email)	Security attestation (ISO 27001, SOC 2 report, or TPN), data processing terms, no training on our data, region, retention, breach notice terms. Robin's written approval
2	Receives customer metadata, personal data or credentials, or can change what we run	Security page reviewed, data processing terms, MFA on our account
3	Receives only public data, or nothing from us	Terms reviewed. Listed here

A new vendor is added to this register before the first call reaches it in any deployed environment. Removing one means removing its secret and its code path.

A customer's own providers. An Org may connect its own model providers (Organisation, Bring your own models): OpenAI, Azure OpenAI, Anthropic, Vertex AI and Gemini, Bedrock, Mistral, ElevenLabs, fal, Replicate or its own endpoint. That provider is the customer's vendor under the customer's own contract, and receives only the jobs the customer routes to it. Its key is encrypted under the Org's own KMS key and shown only by its last four characters.

Register

Vendor	What it does for us	What it receives	Tier
Google Cloud	Cloud Run, Cloud SQL, Cloud Storage, Cloud KMS, Secret Manager, Artifact Registry, Cloud Build, Cloud Logging, Cloud Scheduler, Load Balancing, Transcoder API	Everything	1
fal.ai	GPT Image generation when an openai/ model is chosen	Prompts, and one-hour signed URLs to Org frames and references	1
WorkOS	Sign-in, MFA (set to Required), SSO, organisations, API keys, OAuth for MCP clients	Users' names, emails, passwords, sign-in events	2
Postmark	Receives email sent to project inboxes, forwards to our webhook	Emails and attachments sent to a project	1

Vendor	What it does for us	What it receives	Tier
Resend	Sends invitation, reset and notification email, and Screening Room guest invitations and sign-in links	Recipients' addresses, email bodies	2
GitHub	Source code, CI (GitHub Actions)	Source code, CI logs	2
npm registry	Packages	Nothing. We download	2
ClamAV signature mirror	Virus signatures, fetched at build	Nothing	3
Squarespace	Domain registrar and DNS for final-frame.com	DNS records	2
Google Workspace	Company email (robin@final-frame.com)	Company and customer correspondence	2
Apple Developer	Signing and notarising the Mac app	The app binary	2
TMDB	Title metadata and artwork	Title names and ids	3
OMDb	Title metadata	Title names	3
fanart.tv	Artwork and stills	Title ids	3
EIDR	Title identity registry	Title names and ids, our party credentials	3
Wikidata, Wikimedia Commons	Catalogue spine, images	Ids	3
Open-Meteo	Weather on the My Home page	The user's approximate location, sent from the browser	3

Retired: Firebase Hosting. Its APIs were disabled and firebasehosting.admin removed from the runtime service account on 7 October 2026.

Shared responsibility with Google Cloud

Google is responsible for its data centres, hardware, network and the managed services' underlying security. Final Frame is responsible for IAM, configuration (TLS policy, bucket settings, backups, logging), the application, keys it creates, and who it lets in. Google publishes its MPA mapping and certifications; Final Frame files a copy each year as Tier 1 evidence.

Annual review checklist (Tier 1 and 2)

- Current attestation on file, and its scope covers the service we use
- Data processing terms signed or accepted, with sub-processors listed
- Region of processing and storage
- Retention of our inputs and outputs, and whether they train models
- Breach notification commitment
- Our account: named users, MFA on, keys rotated, unused keys removed
- Still needed? If not, remove the secret and the code path