Flux security and data governance

Your code is private. Here's how we protect it.

Engineering leaders who connect a new tool to their codebase are making a trust decision. Flux exists because engineering leaders need ground-truth intelligence from their codebases, and that intelligence is only valuable if the platform providing it is one you can trust completely. **These are the questions that matter most, answered directly.**

→ Before you connect: questions worth asking

01 How does Flux connect to my repositories?

GitHub App integration. Flux accesses your repository activity — commits, pull requests, repository structure, and metadata — to perform automated code analysis and generate insights. It does not use access tokens that can be lost or leaked, and app permissions are easily reviewable and revocable by the customer. Flux does not modify or write to your repositories, execute code, or require elevated permissions. **Revocable at any time from your GitHub settings.**

02 Does it use my code to train models?

No. Your code is never used to train the underlying LLM (Gemini family models via GCP Vertex AI, which maintains enterprise-grade data governance). Flux uses a **dedicated model per customer** — never commingled.

03 How is my data isolated from other customers?

Per-customer schemas at the database level. All data is encrypted at rest and in transit. LLM context is isolated to your tenant and never persists across requests. All database operations are tenant-aware.

04 Who within Flux can access my code, and when?

Access is strictly limited to operating the service and supporting customers. **All access is logged.** Production infrastructure access requires human-reviewed PRs merged to a protected main branch — **no direct access is structurally possible.**

05 What happens to my code if I stop using Flux?

Customer data is retained for up to **30 days** after contract termination, then securely deleted. System logs stripped of PII are retained for up to 90 days. Retention practices follow **GDPR and CCPA**.

→ Questions worth asking, continued

06	Is the infrastructure auditable?	**Yes.** All infrastructure is defined as Terraform code, version-controlled and human-reviewed. SAST scans all Python and Terraform on every pull request. Comprehensive append-only audit logs cover all significant system events. Annual independent audits, penetration tests, and risk assessments based on CSA CCM, NIST CSF, and OWASP Top 10.
07	Does Flux include contractual confidentiality protections?	**Yes.** Our EULA includes contractual confidentiality protections covering your code, data, and any insights derived from it.
08	What is the incident response policy?	Flux maintains a documented incident response policy covering detection, triage, containment, customer communication, and post-incident review. Customers are **notified promptly** upon discovery and verification, following GDPR and CCPA. Specific notification SLAs are available by negotiation.
09	Is Flux SOC2 or ISO 27001 certified?	We're **building toward SOC2 and ISO 27001** certification. Our systems and processes are designed to meet these requirements — when we pursue certification, it will validate how we already operate. Flux has passed enterprise security reviews conducted by customers in regulated industries, including cybersecurity.
10	Where can I get the full detail?	A complete security whitepaper and a vendor-evaluation checklist are available, covering the framework behind every answer here. **Request both from your Flux contact** or at the address below.

> "Flux gives us ground-truth visibility into what's actually happening in our codebase — without us ever worrying about who else is becoming familiar with the codebase."
>
> Mike Garon · VP of Engineering, Cobalt

Going deeper

For the full security and compliance whitepaper, contact us at info@askflux.ai.

About Flux

Flux is a code-first engineering intelligence platform that helps engineering leaders make better decisions with ground-truth visibility into the work actually happening across today's complex, AI-accelerated codebases.