

Secure development policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	All code and infrastructure definitions for Final Frame
Review	27 October 2027
MPA CSBP	TS-1.13, TS-1.14, TS-1.15, TS-4.0, TS-4.1, TS-4.2, TS-8.0, TS-8.3

Approved by Robin Ashford, Founder, 27 October 2026

Design

- A new endpoint, upload path or integration gets a short threat model in its ADR: what it trusts, what an attacker controls, what stops them.

CI gates

Gate	What it catches
Vendored edit, animation, table, tab strip and layout guards	Silent UI regressions
Database roles created as in production, then migrate and seed	Broken migrations
Unit tests	Permission and domain logic
AXI runner and scoring against a local fake	Scoring logic regressions
Database suites: tenancy first, then the isolation sweep and every other suite	Cross-Org reads or writes, app role privileges, a table carrying with no isolation case
API integration tests, including the route guard	Route behaviour including unauthorised paths. A route that answers signed out, answers another Org's member, or reaches no permission decision, unless listed with a reason
Web build	Build breaks

Results go to the job summary and an artifact:

Gate	What it catches
CodeQL, security-extended queries over the TypeScript	Fails on an error-level finding
gitleaks over the whole history	Any secret not in .gitleaksignore
OSV over	Reported, not gating

Gates outside CI

Gate	Tool	When it runs	Fails on
DAST	OWASP ZAP baseline against QA and the public site, false positives in .zap/rules.tsv with reasons	Weekly (Tuesday) and on demand	A high-risk alert not ignored
Dependency updates	Dependabot: npm, Actions and the API base image, minor and patch grouped, with Dependabot alerts and security updates on in the repository	Weekly (Monday)	n/a
Action pinning	GitHub Actions pinned by commit SHA	n/a	n/a
Internal security review	A review of the platform as a tester would see it, against the penetration test's scope, with findings fixed first	Before each external penetration test	Critical and high findings fixed before the test
Penetration test	An independent CREST-accredited tester, web application, API, MCP and Mac app endpoints	Before production carries a client's production workload, then yearly and after major change	Critical and high findings fixed and retested before go-live

The edge

- The service's own run.app address takes no traffic from the internet.
- A new Cloud Armor rule runs in preview first, and is enforced after a clean preview.

Dependencies

- A new dependency needs Robin's approval.
- Install scripts off in the image.

Code repository

- Private GitHub repository. Access: Robin only.
- MFA on every account with access, enforced by the org 2FA requirement.
- No secrets in the repository. .env is ignored and created from .env.example, which holds no real values. Production secrets live in Secret Manager. gitleaks scans the whole history; a test fixture that looks like a secret is listed in .gitleaksignore with its reason.
- Branch protection on main: required checks, no force push.

Application security requirements

- Input validated by JSON schema on every route.
- Output errors from the error catalogue. Internal detail only in logs.
- No secrets, tokens, cookies, signed URLs or request bodies in logs.
- Rate limits on unauthenticated and sign-in routes.
- Security headers on every response: HSTS, X-Frame-Options, nosniff, referrer policy, and a Content-Security-Policy on every HTML response.
- Every list paginated, maximum 100.

Testing

- A bug fix lands with a test that would have caught it.
- Every Org-scoped table has an isolation test.
- Every route: happy path, unauthorised, one realistic failure.
- Security test results (SAST, DAST, pen test) are kept for two years as evidence.

Environments

- Local: Docker Postgres with the production role topology, seed data only.
- CI: the same, ephemeral.
- The development sign-in exists on no deployed environment.

Final Frame Ltd · Registered in England and Wales · Company number 17413345 · www.final-frame.com/trust