

Information security policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford, founder and security owner
Applies to	Final Frame: the platform, its data, its accounts and everyone who works on it
Review	27 October 2027
MPA CSBP	OR-1.0, OR-2.0, OR-3.0 to OR-3.4

Approved by Robin Ashford, Founder, 27 October 2026

Purpose

Final Frame holds unreleased film and television content for studios and distributors. This policy says how the company protects it. The other policies in this policy set carry the detail. This one says who is responsible and what every other policy must achieve.

Responsibilities

- **Robin Ashford** is the security owner. He approves policies, accepts or rejects risks, owns incident response, reviews access and is the contact for customers and assessors on security.
- **Anyone given access later** (employee, contractor, freelancer) follows these policies, signs a confidentiality agreement before access, and completes security training before access and every year after.
- **Vendors** are held to the Vendor management policy.

What every part of the system must do

1. **Keep each Org's data apart.** Row-level security in Postgres, one bucket and one key per Org. No feature may cross an Org boundary except the platform plane, which is logged.
2. **Decide access on the server, by permission, with default deny.**
3. **Require a second factor** for every person who can reach customer content or production configuration (see the Access control policy).
4. **Encrypt** content at rest and in transit (see the Data classification and handling).
5. **Record** who did what to content in the append-only audit trail, and keep logs long enough to investigate (see the Logging and monitoring policy).
6. **Change the system only through version control and CI** (see the Change management policy, the Secure development policy).
7. **Send customer content to a third party only when listed** in the Vendor management policy and, for models, in the AI use policy.
8. **Be able to recover** within the targets in the Business continuity and disaster recovery.
9. **Delete what is no longer needed** (see the Data retention and disposal policy).

Risk management

- Robin reviews it at least every three months, and fully once a year.
- Each risk has an owner, a decision (fix, accept, transfer) and a date.
- A risk is accepted only in writing, with a reason and a review date.

People

- **Background screening.** Before a person gets access to customer content, check identity, right to work and references, as far as UK law allows. Keep the result on file.
- **Confidentiality.** A signed NDA before access. Reminded at off-boarding.
- **Training.** Everyone with access completes the security awareness module before access, every 12 months, and again when its version changes: phishing and social engineering, handling customer content, signed links, devices and reporting incidents. Developers also cover secure coding (OWASP Top 10). Each completion is recorded with the person, the module, its version and the date.
- **Off-boarding.** Remove access the same day (see the Access control policy).

Contracts

- Customer contracts state the security commitments in this policy set and nothing beyond them.
- Every vendor that handles customer content has terms covering confidentiality, security and data protection (see the Vendor management policy).

Claims

Final Frame does not claim any certification it does not hold. Marketing copy and questionnaires say only what says is true.

Exceptions

An exception to any policy needs Robin's written approval, a reason, an end date and an entry in the risk register.

Approval and versions

Robin approves each policy in this policy set. The approval line in each header names the version approved. Any change to a policy raises its version and needs a new approval line.