

Incident response policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford, incident lead
Applies to	Any event that may affect the confidentiality, integrity or availability of customer content, customer data or Final Frame systems
Review	27 October 2027
MPA CSBP	OR-4.0, OR-1.2, TS-1.5

Approved by Robin Ashford, Founder, 27 October 2026

What is an incident

- Customer content seen, copied or sent by someone not entitled to it, or suspected to be
- One Org able to see another Org's data
- A credential, key, token or signed URL exposed
- An account taken over, or a sign-in nobody can explain
- Malware found in an upload or on a workstation
- A lost or stolen laptop
- A vendor reporting a breach that touches our data
- The platform down, or data lost or corrupted
- Content appearing where it should not (piracy)

Severity

Level	Meaning	Examples
1 Critical	Customer content or credentials exposed, or cross-Org access	Leaked master, bucket made public, RLS bypass, admin account taken over
2 High	Likely exposure, or platform unavailable for customers	Secret in a public place, lost unlocked laptop, outage over one hour
3 Medium	Security control failed, no known exposure	Failed backup, MFA off on an account, malware blocked
4 Low	Weakness found, nothing happened	Vulnerability report, misconfiguration spotted in review

Reporting

Anyone who suspects an incident reports it at once to security@final-frame.com, or to Robin directly. A report is never held back for being unsure. The security awareness module shows what to report and how.

Steps

1. **Detect and log.** Open an entry in the incident log, a private document kept outside the platform: time, who found it, what was seen.

2. **Assess.** Set a severity. Severity 1 and 2: work starts at once, whatever the time.
3. **Contain.** Use the fastest safe action:
 - Disable a user, an API key or an Org.
 - Rotate the exposed secret.
 - Remove a public binding, or disable the key to make a bucket's content unreadable.
 - Roll back to the previous Cloud Run revision.
 - Close any sign-in door involved by removing its secret or setting.
 - Turn a Cloud Armor rule from preview to enforce, or add a deny rule for the source.
 - **Preserve evidence.** Export the relevant Cloud Logging entries and audit rows before log retention removes them. Note every action with its time.
1. **Eradicate and recover.** Fix the cause. Restore data if needed (see the Business continuity and disaster recovery).
2. **Notify.** See below.
3. **Review.** Within 10 working days: root cause, timeline, what changed.

Notification

Who	When	How
Affected customer Orgs (their named security contact)	Severity 1: within 24 hours of confirming it. Severity 2: within 48 hours	Email from Robin, then a written report after review
UK Information Commissioner's Office	Personal data breach likely to risk people's rights: within 72 hours of becoming aware. Final Frame is usually a processor, so the customer as controller decides; we tell them first	ICO breach report
Vendors	When their system is involved	Their security contact
Alliance for Creativity and Entertainment (ACE)	Suspected piracy of a customer's content, with the content owner's agreement	Through the content owner, or ACE directly
Police / Action Fraud	Crime, such as theft of a device	As needed

Testing

A tabletop exercise once a year, and after any major change to the platform. Scenarios to rotate through: leaked signed URL, lost laptop, RLS regression, compromised WorkOS admin, region outage. Record the date and the lessons.