

Workstation security policy

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	Every computer and phone used to build, run or administer Final Frame.
Review	27 October 2027
MPA CSBP	TS-1.3, TS-1.4, OP-2.0

Approved by Robin Ashford, Founder, 27 October 2026

Every Mac

Control	Setting
Full-disk encryption	FileVault on. Recovery key in the password manager, not with Apple
Screen lock	Locks after 5 minutes idle. Password required immediately
Login	A strong account password or Touch ID. No automatic login
Updates	macOS and app updates installed automatically. Security responses within 14 days
Firewall	macOS firewall on, stealth mode on
Malware	Gatekeeper and XProtect on. Software only from the App Store, Homebrew or the vendor's own site
Find My	On, so a lost Mac can be locked and wiped remotely
Backups	Time Machine to an encrypted disk, or none. Customer content never in a backup
Sharing	Screen sharing, file sharing and remote login off unless in use

Robin records the check of every item above once a quarter, with the access review.

Accounts and credentials

- A password manager holds every password, recovery code and API key used by hand. Its own MFA is on.
- MFA on every account that can reach production or customer data: Google, GitHub, WorkOS, Postmark, Resend, fal, Squarespace, Apple Developer, the password manager.
- Prefer passkeys or a hardware key over app codes, and app codes over SMS. No SMS where a better factor exists.
- Production secrets are not stored on disk. The root .env holds local development values only.

Shared machine, several companies

These Macs also hold credentials for other projects and companies. Rules that keep them apart:

- Never copy Final Frame data or secrets into another project's tools, buckets or databases, and the reverse.

Customer content on a workstation

- Not stored by default. When a task needs a file locally (debugging a transcode, for example), keep it in one working folder and delete it when the task ends.
- Never on removable media, personal cloud storage or a phone.
- The Mac app's transfer journals hold part lists and offsets, not content.

Phones and tablets

- Used as an authenticator only. Passcode and biometric lock on, OS updated, Find My on.
- No customer content, and no admin sessions to the platform, on a phone or tablet.

AI coding assistants

They run on these Macs with Robin's permission settings. They follow the AI use policy: no customer content, no secrets pasted in, production changes only through the Change management policy.

Loss or theft

Report it as an incident at once (see the Incident response policy): lock and wipe with Find My, revoke the Mac's sessions and tokens (Google, GitHub, gcloud, WorkOS), rotate any secret it could read.

Remote work

All Final Frame work is remote. Work only on trusted networks, or on public Wi-Fi with every connection over TLS. Keep screens out of view of others when customer content is open.