KlipLoft
Clipboard manager for macOS · getklip.me

SECURITY REVIEW REQUEST

Approving KlipLoft on company Macs

With the configuration in this document, KlipLoft keeps a local clipboard history that never leaves the Mac, filters out credentials before they are saved, and overwrites what users delete. It replaces habits that are riskier than it is.



Version
KlipLoft 1.70 (build 76)

Platform
macOS 26 or later

Signing
Apple Developer ID, notarized

Developer team ID
2QJBT9C4Q7

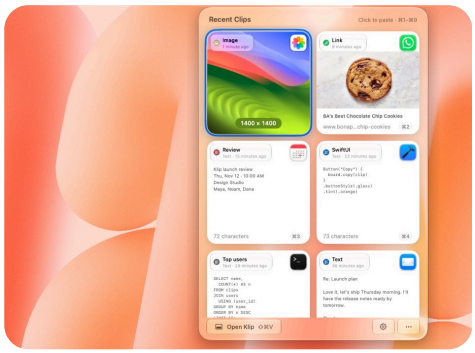
Summary

KlipLoft is a local clipboard history for macOS. Configured as described here, nothing leaves the Mac, secrets are filtered out before they are saved, and deleted data is overwritten.

1 It reduces an existing risk

Without a clipboard manager, people keep reusable values wherever they can copy them again: Notes, Stickies, text files on the Desktop, Slack messages to themselves, open browser tabs. Those places sync to third-party clouds, never expire and never filter secrets.

KlipLoft keeps the same values on the local Mac, removes old clips automatically, and refuses to store credentials.



Recent clips under KlipLoft's menu bar icon

2 Data never leaves the Mac

- **Storage:** the history lives in the user's Application Support folder. On a FileVault-encrypted Mac it is encrypted at rest and readable only by that user account.
- **No accounts or servers:** there is no KlipLoft account, no KlipLoft server and no analytics service.
- **iCloud sync (optional):** uses Apple's CloudKit and the user's own private iCloud database. It will be **turned off**.
- **Other network requests, both of which can be turned off:** an update check that downloads a small version file from getklip.me, and link previews, which fetch a copied link's title and image.

3 Credentials are kept out of the history

- **Never saved:** copies from Apple Passwords and Keychain Access, from browsers' built-in password manager pages, and copies that password managers mark as concealed or transient, including 1Password.
- **Secret filter:** "Don't Save API Keys and Tokens" skips any copy containing GitHub, GitLab, AWS, Slack, OpenAI, Anthropic, Stripe, Google or npm keys and tokens, Slack webhook URLs, JWTs, or PEM and PGP private keys.
- **Automatic copies:** copies an app makes by itself, such as copy-on-select in terminals, are not saved by default.
- **Ignored apps:** copies from any app IT designates can be blocked completely.

4 Retention and deletion

- **Automatic removal:** history is pruned after a day, a week or a month, and users can clear it at any time.
- **Secure erase:** when on, deleted clips' text and images are overwritten so they can't be recovered from the disk.

5 No leaks while presenting

With "Show During Screen Sharing" turned off, KlipLoft's windows are hidden from screen shares and recordings, so a clipboard history can't appear by accident on a customer call.

6 Trusted distribution

- **Signed and notarized:** signed with an Apple Developer ID (team 2QJBT9C4Q7) and notarized by Apple. Gatekeeper reports it as "Notarized Developer ID".
- **Installation:** from the DMG on getklip.me or through Homebrew (`brew install --cask ronier83/tap/kliploft`), with a checksum published for each release.

7 Known risks and how they're handled

Risk	Mitigation
iCloud sync is on by default	Turned off, and could be enforced with a configuration profile
The API-key filter and secure erase are off by default	Both turned on
Not sandboxed, and needs the Accessibility permission to paste	Standard for clipboard managers; the app is signed and notarized, and the developer is available for review
A single developer, no vendor support contract	The developer is the employee making this request and can answer technical questions directly
History is not encrypted by KlipLoft itself	Protected by FileVault and the macOS user account; history is pruned and secure erase is on

8 Required configuration

All settings are standard macOS preferences in the `com.ronerez.Klip` domain.

Setting	Value	Effect
`iCloudSync`	**NO**	The history stays on this Mac
`skipSecrets`	**YES**	API keys, tokens and private keys are never saved
`secureErase`	**YES**	Deleted clips are overwritten
`showDuringScreenSharing`	**NO**	Hidden from screen shares and recordings
`linkPreviews`	**NO**	No outbound fetches for copied links
`historyCapacity`	**1**	History is kept for one week
`ignoredApps`	**list**	Passwords, Keychain Access, plus internal tools IT designates

Request

Approve KlipLoft 1.70 for installation on my work Mac, with the configuration above.

Facts in this document are taken from KlipLoft's source code and the signed 1.70 build. Enforcing the settings with a configuration profile should be confirmed on a test Mac before rollout.