How FiduKit protects your data

Last reviewed 20 November 2026.

Local processing, nothing uploaded

- Statement PDFs are read, categorized, balanced and filled into the court forms **inside the browser**. No FiduKit server ever does that work.
- Statements, transactions, balances, categories and account numbers are **never sent to FiduKit**. Our servers have no place to store them.
- Work in progress, including the original statement PDFs, is **saved in the browser's storage on that computer**. FiduKit adds no encryption of its own there, so we recommend full-disk encryption (BitLocker or FileVault) and a browser profile nobody else uses.
- **Error messages stay local.** An error is written only to the browser's own console, with figures, email addresses and file names taken out, and no error-reporting service receives it.

Strict browser security rules

- The app tells the browser it may connect to **app.fidukit.com and nowhere else**, so the browser itself blocks any request to another site.
- No analytics, advertising, session-recording or AI service **can load in the app** or on this website.
- When you pay, you leave the app for **Polar's own checkout page** as an ordinary page change. The app itself never talks to a payment service.
- To see it for yourself, follow the Network-tab check on the privacy page while you prepare an accounting.

Encryption and sign-in

- Every connection uses **HTTPS**, and browsers are told never to fall back to an unencrypted one.
- **Passwords are never stored in readable form.** Each one is salted and hashed with a deliberately slow one-way method, so it can't be turned back into the password.
- Sign-in, sign-up and password-reset attempts are **capped** to stop password guessing. Past the cap, further attempts are refused for a while.
- A link to reset a password or change an email address **expires after 15 minutes**. The sign-up confirmation link expires after 24 hours.
- The **sign-in cookie** can't be read by scripts on the page and travels only over HTTPS. It ends 90 days after sign-in at the latest, and "Sign out of all devices" ends every session at once. Each request that changes something carries an anti-forgery check.
- With **Google sign-in** we keep your email address, name and Google account ID. We never keep a Google access token.
- **Backups are encrypted** in the browser with AES-256, under a passphrase you choose. We never see the passphrase and can't recover a lost one, and a file that has been altered refuses to open.

Minimal data on our servers

- Our servers keep **only what an account needs**, which is sign-in details, purchases and a dated record of each download request. The privacy page lists it in full.
- **An automated check keeps it that way.** If the server's records gain any field outside an approved list, the release fails before it can ship.
- **Server logs** record security and billing events, such as a failed sign-in, without passwords, statements or figures.
- Polar takes payment as **the merchant of record**. Card details never reach FiduKit, and Polar never sees a statement, a transaction or a conservatee's name.

Account numbers on court forms

- On the GC-400 forms FiduKit fills, account numbers print as **the last four digits only** (California Rules of Court, rule 1.201(a)(2)), for example `••4321`.
- Check, reference and trace numbers are **left as printed**.
- The statements attached under Probate Code §2620(c) are **your bank's own PDFs** and usually show full account numbers. The app tells you this and points you to your court's rules.
- Your working papers (CSV and Excel) and the backup file are your own records and **aren't masked**.

Account deletion

- Deleting an account removes it, its email links and its sessions **immediately, in one step**.
- **Purchase records** are kept for tax and accounting, unlinked from your name.
- Work saved in **your browser** isn't touched, so delete it there yourself.

What we don't offer

We have **no SOC 2 report, no ISO 27001 certification and no third-party penetration test**. There's also no single sign-on (SAML) and no on-premises version. The client data a firm worries about never reaches us, by design. We're happy to answer a security questionnaire by email.

Reporting a security issue

Email support@fidukit.com and describe what you see. Please never attach client data. The privacy policy covers retention and your rights.

FiduKit is document-preparation software, not a law firm. We give no legal advice and file nothing with any court. You review, sign and file your own accounting (California GC-400 series, Probate Code §2620). FiduKit is not affiliated with or endorsed by the Judicial Council or any court. Consult an attorney about your case.