COMPANY
REFI2 Labs Inc.

OFFICE
100 King St W, Suite 6200
1 First Canadian Place
Toronto, Ontario M5X 1B8, Canada

CONTACT
+1 (905) 536-6968
info@refi2.com
refi2.com

How REFI2 Keeps Your Data Safe

Everything you upload, sign, or share on REFI2 is encrypted, visible only to the people you choose, and protected against tampering. This page explains how in plain words. Security teams who want the cryptography, protocols, and compliance mapping can read the REFI2 Security Architecture.

Your data is encrypted

When your browser talks to REFI2, the connection is locked with TLS 1.3, the same standard online banks use. Older, weaker versions of the protocol are refused, and your browser is told to never connect to us without encryption. Anyone listening on the network, including public Wi-Fi, sees only scrambled bytes.

Files you store with us are encrypted on disk with AES-256, a cipher approved for classified government data. Your password is never stored at all, only a one-way fingerprint of it, so even we cannot read it. The most sensitive secrets, such as two-factor codes and document passwords, get a second layer of encryption with keys kept away from the database. A stolen copy of the database would not be enough to open them.

Who can see your data

Your data is visible only to people who need it. Every page and every request checks who you are before anything is shown, and every investor account requires a second login step, such as a passkey or a one-time code, on top of the password.

Shared documents go out through personal links. A link can require the viewer’s email, expire on a date, block downloads, ask for an NDA before opening, and stamp the viewer’s name across the pages. Download links themselves stop working after one hour.

Our own team sees personal details masked by default, like “M. W.” instead of a full name. Opening a full record is a separate step that gets logged. The highest level of administrative control requires several team members to approve together, so no single person, and no single stolen laptop, can take it over.

Every quarter we go through who on our team has access to what, name by name, and access is removed the same day someone leaves.

Signed documents cannot be secretly changed

When everyone has signed, the final PDF gets a digital seal. Change a single character afterwards and any PDF reader will flag the document as modified. The seal also carries a timestamp from an independent authority, which proves exactly when the document was finalized.

The signing process records who opened the document, who signed, when, and from where. Each entry is chained to the one before it, so deleting, editing, or backdating an entry breaks the chain and is caught.

Where it runs

REFI2 runs entirely on major cloud providers that are audited by independent accounting firms every year. Data centers, hardware, and network security are handled by companies whose controls are checked under SOC 2 and ISO 27001.

WHAT THEY DO FOR US	THEIR SECURITY AND AUDIT PAGE
Website hosting	Vercel
Application hosting and databases	Railway
Network protection and file storage	Cloudflare
Account login	Clerk
Database	Turso
Sign-in with Google and key protection	Google Cloud
Encrypted backups	AWS

If something goes wrong

A copy of our databases is made every day, encrypted, and stored with a separate cloud provider. In the worst case we lose at most one day of data and are back online within four hours.

Our systems are watched around the clock by automatic alerts. If a security incident ever affects your data, we tell you within 72 hours of confirming it.

To report a security problem, write to security@refi2.com. Reports go straight to the engineering team.

How long we keep your data

DATA	HOW LONG
Identity checks and signed agreements	5 years after you stop using REFI2, as financial regulations require
Everything else about you	Deleted within 30 days if you ask, unless the law says we must keep it
System logs	1 year
Backups	30 days, so deleted data is gone from backups too

SOC 2

SOC 2 is a security standard from the American Institute of CPAs. It asks whether a company protects customer data with real controls such as encryption, access limits, change tracking, and careful vendor selection. An independent auditor then checks those controls and writes a report.

REFI2 is built to the SOC 2 criteria for security, availability, and confidentiality, and every provider we rely on already holds its own SOC 2 report. The REFI2 Security Architecture maps each control to the SOC 2 criterion it covers, so your security team can review it today.