REKEY · FREE CHECKLIST

AI Key Lockdown Checklist

How to rotate API keys after a breach, and lock them down so the next one does less damage. Ten steps, in order, written for small teams without a security person.

In October 2026, Railway told all users to rotate their secrets, OpenCode lost customers' AI API keys, and a poisoned LiteLLM release stole credentials. If a provider has just told you to rotate your keys, start with steps 1 and 2.

1 Find every place your keys live

You can't rotate a key you forgot about. Keys spread across your hosting provider's environment variables, CI secrets, local .env files, and hosted AI tools that store a key on your behalf.

Do this: Make a list of every AI and API key with three columns: what it's for, where it's stored, and who can see it.

2 Rotate the right way

Removing a key from your code doesn't stop anyone who already copied it. If a key may have leaked, revoke it first and accept a few minutes of downtime.

Do this: For each key on your list: revoke it at the provider that issued it, create a new one, update it everywhere it's used, and redeploy.

3 Set hard spend limits and usage alerts

A stolen AI key is usually used to run up your bill. A hard limit caps the damage, and an alert tells you something is wrong before the invoice does.

Do this: At every AI provider you use, set a hard monthly spend limit just above your normal usage, plus an alert at about half of it.

4 Use one key per app and per environment

When every app, environment and teammate shares one key, a single leak exposes all of it, and you can't rotate it without breaking every app at once. Small, separate keys keep a leak small.

Do this: Create a separate key for each app and each environment (dev, staging, production) with the smallest scope that works, and delete any key you don't use.

5 Keep keys out of frontend code and public repos

Anything shipped to the browser can be read by anyone, including env vars with prefixes like NEXT_PUBLIC_ or VITE_. Keys committed to git stay in the history even after you delete the file.

Do this: Move secret keys behind a server route, then scan your full git history with a secret scanner such as gitleaks or GitHub secret scanning, and rotate anything it finds.

6 Turn on 2FA everywhere that matters

Your hosting, GitHub, AI provider and domain registrar accounts can each hand an attacker your keys or your traffic. A password alone isn't enough for any of them.

Do this: Turn on 2FA with a passkey or an authenticator app (not SMS) on all four, and store the recovery codes somewhere safe and offline.

7 Pin your AI libraries

In October 2026 a poisoned LiteLLM release stole credentials from machines that installed it. Pinned versions and a lockfile mean a bad release doesn't reach you automatically.

Do this: Commit your lockfile, pin exact versions of AI libraries and SDKs, and read the changelog before upgrading, ideally a few days after a release comes out.

8 Give AI agents and MCP tools the least access possible

Coding agents and MCP tools can read files, run commands and call APIs with whatever credentials you give them. If they hold your production keys, a bad prompt or a malicious tool can use them too.

Do this: Give agents their own credentials with no production write access, and require your approval before destructive actions like deleting data, deploying or running migrations.

9 Check usage dashboards weekly

Spend limits stop the worst case, but a slow leak can run for weeks under the limit. A quick weekly look catches usage you don't recognize.

Do this: Set a weekly 5-minute reminder to check each AI provider's usage dashboard, and turn on spike or anomaly alerts where the provider offers them.

10 Write a 15-minute “keys leaked” plan

When a provider tells you to rotate everything, you don't want to work out the order under pressure. A one-page plan turns a stressful day into a checklist.

Do this: Write down who rotates which key, in what order (most powerful first: cloud, payments, AI providers, then the rest), and every place each new key has to go.

Want a hand with it?

In a 90-minute AI Stack Lockdown session we work through this list together in your accounts, and you leave with a short written summary.

Email me, or book a free 15-minute Zoom call:
adrian@rekeysecurity.com
rekeysecurity.com/#contact