Security policy

Last updated 27 October 2026

- This is how we keep Veurone Studio and your data safe. It covers the app, studios on the web, learn.veurone.com, watch.veurone.com, veurone.com and the accounts that run them.
- Veurone is a one-person company. Its owner wrote and approved this policy, follows it, and reviews it every year and after any big change or incident.
- It backs our answers to the Cloud Security Alliance's questionnaire (CAIQ v4.1), listed in CSA's STAR registry. No outside auditor has checked it.

1. How this policy works

- Veurone's owner is responsible for security and privacy, approves this policy and its changes, and checks once a year that it's followed.
- We keep private security records: what we run and hold, our suppliers, risks, access reviews, incidents, exceptions and each yearly review.
- Any exception to this policy is written in those records first, with the reason, the risk and an end date. In an emergency, it's written down the same day.
- Anyone else who ever works on Veurone reads and agrees to this policy before they get access.
- Once a year, and before big changes, we list the risks to Veurone Studio and your data, how likely and how serious each is, and what we do about it.

2. People

- Today the owner is the only person with access to Veurone's systems and your data.

- Anyone else gets access only after signing a confidentiality agreement and agreeing to this policy, gets only what their work needs on an account of their own, and loses it the day the work ends, when they return or delete any Veurone data they hold.
- The owner takes a security awareness refresher every year, and follows the security notices of the services Veurone runs on.

3. Accounts and access

- Every account that runs Veurone (code, hosting, database, email, payments, domains) has two-step sign-in and a unique password kept in a password manager.
- Each person and service gets only the access it needs. Service keys live in each provider’s secret store, never in code, chats or documents.
- Every three months we review who and what has access to each service, remove what isn’t needed, and record the review.
- Our admin dashboard is open only to named staff. It can read an account’s work to help and keep Veurone Studio safe, never change it, and each look is recorded and kept for a year.
- You sign in with a one-time code we email you, or with Google or Microsoft. Row-level security on every database table means each account reaches only its own data, and each team only its own learners.

4. Your data

- We sort data three ways: public (what you publish), customer data (your projects, your learners’ records and any personal data), and secrets (keys and passwords). Customer data and secrets are never public.
- Our records list the data we hold, where it’s stored, where it flows and who looks after it. We review them every year and when something changes.
- We use your data only to run Veurone Studio for you, and never to train AI models. Testing uses test data in a separate staging project, never copies of yours.
- We keep and delete data as the Privacy Policy says. When you close your account, we delete your data within 30 days.
- If an authority asks us for your data, we give it only when the law requires it, tell you first unless the law forbids it, and give as little as we can.

How we handle personal data for you is set out in our data processing agreement and Privacy Policy.

5. Encryption

- Every connection uses HTTPS. Plain HTTP is turned away or sent to HTTPS.
- Our providers encrypt everything they store, using their own audited key management. Studios on the web have encrypted disks.
- We hold no keys that encrypt your stored data. Our own service keys are replaced when they expire, when anyone with access leaves, and at once if one may have leaked.

6. Building and changing Veurone

- All code is kept in private GitHub repositories, and every change is a recorded commit.
- Automated tests run before each release. Database changes are numbered migrations, tried on a separate staging project before production.
- Security is part of the design: row-level security on every table, rate limits on sign-in and learners' endpoints, input checks, and no secrets in code.
- If a release goes wrong, we go back to the last good version: the websites and workers keep earlier versions, and the app and cloud are rebuilt from Git.
- An urgent fix can skip the usual steps, and is written down the same day.

7. Vulnerabilities

- GitHub checks our code's dependencies for known vulnerabilities, and we check them again before each release.
- We fix critical and high-risk vulnerabilities within 14 days, and others within 90.
- We answer a security report within three working days, and tell the person who sent it when it's fixed.
- No outside company has tested Veurone for vulnerabilities yet.

Report a security problem to info@veurone.com, as our security.txt says.

8. Infrastructure

- Veurone Studio runs on managed cloud providers: Cloudflare, Supabase and Fly.io. They secure the data centres, hardware, networks and operating systems, and are audited for it.
- Each studio on the web is a private machine of its own, with no public address.
- Staging and production are separate. Only HTTPS endpoints are open to the internet.

9. Logging and monitoring

- Our providers log access and errors. Our own logs record each admin look and each error report.
- Error reports have names, email addresses and file paths taken out, are deleted after 90 days, and are read at least every week.
- Our cloud’s health is checked every 30 seconds. Clocks come from our providers’ time servers.

10. Incidents

- If something goes wrong, we stop it spreading, find out what happened and whose data it touched, and fix it.
- If it affects your data, we tell you without undue delay, with what we know and what we’re doing about it.
- Every incident is written down with what we learned, and we check the steps once a year.

11. Continuity and backups

- In the app, your projects are files on your computer, and they sync to your account. You can keep working if our cloud is down.
- Our code is on GitHub and on the owner’s computer. Every week, the database is exported to encrypted storage away from Supabase.
- Our records say how to bring each part back if a provider fails, and we walk through it once a year.

12. Suppliers

- We prefer suppliers that are independently audited for security, and work with each under its data processing terms. Where one isn’t audited, we record why we use it and give it as little data as we can.
- Our records list each supplier, the data it gets, where, and its audits. We review the list every year.
- We tell you at least 30 days before we add a company that handles your personal data, as the data processing agreement says.

13. Devices

- Computers used for Veurone have disk encryption, a screen that locks at once, automatic updates, the system’s own malware protection and a firewall.
- Veurone is worked on from a private room, and a computer left alone locks.
- If a computer is lost or stolen, its disk stays encrypted and we replace every key it held. Before we give one away, we erase it.
- We don’t move customer data on USB drives or other removable media.

14. What’s yours to do

- Choose who’s on your team, and remove people who leave.
- Decide what you publish and share, and which learners’ details you collect.
- Keep the email accounts you sign in with secure, with two-step sign-in where you can.

For questions about this policy, email info@veurone.com.