
Security

Last updated August 8, 2026

Web version: noctic.ink/security. This PDF was made on October 16, 2026 from the text published there; later changes appear on the web page.

How the system is built

- All traffic is served over encrypted transport with strict transport security enforced.
- Passwords are hashed with a slow, salted key-derivation function. We never store or log a plaintext password.
- New passwords are checked against known breach corpora using a hash-prefix lookup, so the password itself never leaves the browser.
- Row-level security governs every table, and sensitive columns are revoked from ordinary roles rather than filtered in the client.
- Server functions validate an authenticated token on every privileged call, with per-account and per-address rate limits.
- Model provider keys exist only in server-side secrets. They are never embedded in a page or bundle.
- Administrative actions are recorded with an attributable audit history.

Reporting a vulnerability

Send reproduction steps, affected endpoints and impact to the security contact on the [Contact](https://noctic.ink/contact) (noctic.ink/contact) page. Please give us reasonable time to fix an issue before disclosing it, avoid accessing other people's data, and do not run denial-of-service or automated scanning against production. We will not pursue researchers acting in good faith under these conditions.

Out of scope

Missing best-practice headers with no demonstrated impact, self-inflicted issues requiring a compromised device, social engineering of our staff, and reports produced solely by automated scanners without a working proof of concept.

What to expect from us

First reply

Same day, including weekends, from a person rather than an automatic acknowledgement.

Assessment	Within three working days we confirm whether we could reproduce it and how we are rating the impact.
Critical issues	Mitigated immediately, ahead of anything else in progress.
Updates	You hear from us while it is open, not only when it is closed.
Credit	Public thanks if you want it, silence if you would rather not be named.
Good faith	We will not pursue legal action against researchers who follow the conditions above.

Special care around students

Cadence holds data belonging to minors. Please do not test against real school accounts, real student data or a live campus. If a vulnerability can only be demonstrated that way, tell us what you believe is possible and we will reproduce it ourselves on a test campus rather than asking you to.

If something goes wrong

In the event of a breach affecting personal data we notify affected people directly and without delay, notify the relevant supervisory authorities within the period the law requires, tell the schools involved before we tell anyone else, and publish a plain-language account in the [Newsroom](https://noctic.ink/newsroom) (noctic.ink/newsroom) once people have been informed. We would rather publish an uncomfortable summary than a vague one.

What we ask of you

- Use a strong, unique password. We check new ones against breach corpora, but that is a floor, not a wall.
- Keep client secrets on your server. Anything shipped to a browser is public, whatever the file is called.
- Review connected apps occasionally and revoke what you no longer use.
- Treat any message asking for your password, a full API key or a session token as fraudulent. We will never ask for them.

Copyright 2026 Noctic™. All rights reserved. Noctic, Shiba AI, Cadence and Noctic Compass are trademarks of Noctic.