Jura

SECURITY AUDIT

How Jura protects you, checked line by line.

A review of the code that actually ships — what it guarantees, and, in the same breath, what it does not.

DATE	SCOPE	AUTHOR
15 September 2026	Jura app 2.4.0 (76) · Jura API	Jura engineering (first party)

Why this document exists

Read before you trust us

Most apps ask you to trust a sentence. This document tells you what the software does, where it is strong, and — just as plainly — where it is not. Every claim below corresponds to code in the running system. The honest limits are printed beside the guarantees they qualify, not buried beneath them.

Jura is a dating and rishta app, which means it holds the two things people are most careful with: their face and their conversations. The sections that follow describe exactly how each is handled, in the order a cautious person would ask.

How to read this

The summary overleaf grades each area with one of four marks. They mean different things, and the last is not a softer way of saying the first.

STRONG	The protection is implemented, and it does what the sentence beside it says.
NONE PRESENT	The risk does not exist here, because the thing that creates it is not installed at all.
CONSTRAINED	A power we hold over your data, deliberately narrowed and logged.
STATED LIMIT	A real limitation. Not a weakness we are hiding — a boundary we are telling you about, with the reason.

What is inside

At a glance

Summary of findings

WHAT WE CHECKED	FINDING	STATUS
Passwords	Never stored. Hashed with PBKDF2-SHA256 at 500,000 iterations, each with its own random salt.	STRONG
Messages at rest	Encrypted with AES-256-GCM before they touch a disk. A stolen database is unreadable.	STRONG
End-to-end encryption	Not implemented, by choice — reported conversations must be readable by moderation.	STATED LIMIT
Chat photos	Deleted from storage 72 hours after upload, permanently, by an automatic hourly sweep.	STRONG
Photo access control	A photo sent in one conversation cannot be opened by anyone outside that conversation.	STRONG
Your location	Coordinates are never sent to another member. Distance is deliberately coarsened.	STRONG
Face verification	A live, server-authorised check. It raises the cost of impersonation; it does not make it impossible.	STATED LIMIT
Moderator power	One account. It can read a reported conversation and nothing else, and every use is logged permanently.	CONSTRAINED
Account deletion	Immediate and real: photos removed from storage, account row deleted.	STRONG
Tracking and advertising	No analytics SDK, no advertising SDK, no third-party tracker in the app at all.	NONE PRESENT
Abuse limits	Every expensive action is rate-limited per member — a damper on abuse, not a hard wall.	STATED LIMIT

Sign-in

Your account

Your password is never stored anywhere, in any form you could read. It is put through PBKDF2-SHA256 **500,000 times** with a 16-byte random salt unique to you, and only the result is kept. Two members with the same password produce completely different stored values, and working backwards from the stored value to the password is not practical.

If you sign in with Google instead, Google confirms who you are and Jura never sees a password at all.

Your session is a signed token that expires after 60 days and carries its own unique id. Signing out revokes that specific token immediately — it stops working even though it has not expired.

Conversations

Your messages

Every message body is sealed with **AES-256-GCM** before it is written, each with its own random nonce, and stamped with a version so the key can be rotated without losing anything. The key lives only in the server's secret store — never in the database, never in the app. If someone walked away with a complete copy of the database, they would hold ciphertext.

The encryption is proved every time the service reports its health: the system encrypts a known phrase, decrypts it again, and refuses to report itself healthy if the round trip fails.

> **The limit, plainly:** this is encryption at rest, not end-to-end encryption. The server holds the key, so the server can decrypt. That is a deliberate trade: on a platform where people meet strangers, a report of harassment has to be readable by a human, or the report is worthless. If you want a channel nobody but you and one other person can ever read, Jura is not that channel and does not pretend to be.

Images

Your photos

— **Profile photos** stay while your account does.

— **Photos sent in chat**, **verification selfies** and **photos on public Occasions** are given an expiry of 72 hours at the moment they are uploaded. An automatic sweep runs every hour, deletes the expired objects from storage, and marks the record. After that the image is gone — not hidden, not archived. Requesting it returns "this photo expired" to everyone, including us.

— Chat photos and verification selfies must be taken live in the app. The app offers no way to choose an old picture from your camera roll.

— The one selfie that earned a verification badge is kept while that badge stands, because later photos are quietly compared against it. It is deleted when the badge is removed or a newer one replaces it, and it is never shown to another member.

Who can open a photo

Private images are not simply hard-to-guess links. Every request is checked against who you are: you can open your own; a photo sent in a conversation can be opened by the person it was sent to *in that conversation* — not by the sender's other matches, and not by anyone else on Jura.

> **The limit, plainly:** nothing can stop a person who receives a photo from screenshotting it. The 72-hour rule governs Jura's storage, not someone else's phone.

Distance

Your location

If you allow location access, your coordinates are stored so the app can say how far away someone is. **Your coordinates are never sent to another member.** What they see is a distance that has been deliberately blunted: never finer than a mile, and beyond ten miles rounded into five-mile steps.

That rounding is not cosmetic. A precise distance, read from two or three places, can be turned back into an address. A coarse one cannot. You can also turn distance off entirely in Settings, or refuse location access — the app works without it.

Identity

Face verification

Verification runs live, in the app. On most phones the camera watches while you follow a short sequence in a random order — look straight, turn, blink, smile — so a printed photo or a replayed video does not pass. The captured face is then compared with the faces already on your profile, and the badge is granted **only** on a positive match; every other outcome, including "unclear", grants nothing.

Two details worth knowing. First, the upload must be authorised by a ticket the server issued moments before — one ticket, one selfie, ten minutes — so a stolen access token and a command line cannot mint a badge without the app. Second, if the matching service is unreachable, verification **fails closed**: no badge. A checker that grants badges when it is broken is worse than no checker.

> **The limit, plainly:** no single frame can prove to a server that a living person was in front of the camera. A determined person running a modified app remains possible. Treat the badge as strong assurance that the person in those photos took a live check — not as absolute proof of identity. And when a new profile photo does not match the verified face, Jura does not block it; unreliable matching on ordinary photographs (sunglasses, a side profile, an old picture) would punish honest members far more often than it would catch a dishonest one. It goes to a person in the moderation queue instead, and you are told it happened.

Oversight

Moderation, and the power we hold

There is exactly one moderation account. It can see reports, ban, and remove accounts. It can read **the conversation attached to a report, and only that conversation** — there is no route in the software that lets anyone browse private chats at will. Every moderation action, including every time a reported conversation is opened, is written to a permanent audit log that is never edited or erased.

Leaving

Deleting your account

Settings › Account › Delete my account is not a flag on a row. Your images are deleted from storage in batches, and your account record is then deleted outright — profile, photos, matches and messages with it. Records of moderation actions remain, as an audit trail; they are what makes the paragraph above verifiable.

What we are not doing

Tracking, advertising, data selling

The app ships with no analytics SDK, no advertising SDK, and no third-party tracker of any kind. Nothing measures you for a marketing company, because nothing of that sort is installed. We do not sell data and we do not show ads.

The permissions the app asks for are short and each has an obvious purpose: internet, camera (photos and verification), and location (distance, optional). Microphone access is **explicitly removed** from the app at build time — Jura cannot record audio even by accident.

Infrastructure

Where it runs

Jura runs on Cloudflare: the API on Workers, profiles and messages in D1, images in R2, live chat on Durable Objects. Face matching runs on a private Jura service that images pass through for comparison and which does not retain them; it is reached over a short-lived signed link, never with your session. Transport is HTTPS throughout.

Abuse

Rate limits

Expensive or abusable actions are capped per member, per window — verification attempts (6 an hour), photo uploads (60 an hour), messages (600 an hour), Occasions posts (5 a day), searches, and more.

> **The limit, plainly:** these counters are a cost-and-abuse damper, not a security boundary. Counter reads can lag by up to a minute, so a hard burst can overshoot a cap before it catches up. They exist to stop loops and expense, and the code says so in as many words.

Evidence

Testing

The backend ships with an automated test suite — **69 tests across 4 suites, all passing** — covering the cryptography, the encryption round trip, liveness tickets, face verdict handling, distance maths, request handling and Occasions rules. The code also type-checks clean before every deploy. Tests are not proof of security; they are proof that the parts described in this document behave as described, every time they change.

Disclosure

What this document is not

This is a first-party audit: our own review of our own code, published so you can hold us to it. It has not been carried out by an outside security firm, and we are not going to imply otherwise. If that changes, this document will say so, with a date and a name.

Verification

Check some of it yourself

— The app's requested permissions are listed on its store page. Compare them with the short list in this document.

— The service reports its own health, including a live self-test of message encryption, at /v1/health.

— Send yourself a photo in a chat and try to open its link 72 hours later. It will be gone.

— Delete a test account, then try to sign in to it.

Found a hole?

Tell us before you tell anyone else and we will work with you, thank you publicly if you want that, and fix it as fast as we can: support@jura.best. We will not threaten anyone who reports a vulnerability in good faith.

This document is reviewed whenever the security-relevant parts of Jura change, and the date on every page is updated when it is. The current version always lives at jura.best/security.html, alongside the Privacy Policy and Terms.