NexaPair security white paper

Kayak Strategic Advisors Private Limited · version 04 November 2026

This paper states what is true of NexaPair's security today. Every control is marked Live, Roadmap or To be confirmed. Items in square brackets are being finalised; we do not describe them until they are.

Standards

Controls are aligned to ISO/IEC 27001 and SOC 2. Certification is not yet held, and we do not claim it.

Controls

Role-based access (RBAC) [Live]
Five roles decide who sees and changes what; API keys are scoped the same way.

Tenant isolation [Live]
Every record carries its organisation, and every query is filtered by it.

Audit trail [Live]
Who changed what, and when, exported to CSV or JSON.

Export and portability [Live]
Ten registers export to CSV and JSON at any time, audit trail included.

Secrets: AI provider keys [Live]
Encrypted with AES-256-GCM; personal data is removed before any AI call.

UAE data residency [Live]
Deployable in a UAE cloud region, so records can stay in the country.

Signed webhooks [Live]
HMAC-SHA256 signature with a timestamp on every event.

Encryption in transit and at rest [To be confirmed]
TLS in transit; at-rest encryption by the hosting provider. Details: [ENCRYPTION DETAILS].

Vulnerability management [Live]
Code, dependency, secret, container and web scanning on every change and weekly, with automatic update pull requests. Penetration test: [PENETRATION TEST DATE].

Single sign-on: OIDC and SAML [Live]
Sign in with Entra ID, Okta, AD FS or any OIDC or SAML 2.0 provider, with group-to-role mapping.

UAE PASS sign-in [To be confirmed]
Built and switched off until each organisation completes UAE PASS onboarding with TDRA.

Multi-factor authentication [Live]
Authenticator-app codes, passkeys and recovery codes, enforceable per organisation, role and duty.

SCIM provisioning [Roadmap]
Users and roles kept in step with your directory.

AI governance

Personal data is removed before any request reaches an AI model. AI outputs are labelled and logged, and a person makes the decision. Customer-supplied AI provider keys are encrypted with AES-256-GCM.

Still being finalised

Certifications: Not yet held · aligned to ISO/IEC 27001 and SOC 2

Hosting provider and region: [HOSTING PROVIDER]

Encryption at rest and in transit: [ENCRYPTION AT REST AND IN TRANSIT DETAILS]

Latest independent penetration test: [PEN-TEST DATE] · [PEN-TEST FIRM]

Sub-processors: [SUB-PROCESSOR LIST]

Data processing agreement: [DPA TEMPLATE]

Data retention and deletion: [DATA RETENTION POLICY]

Contact

Audit and security questions: [AUDIT CONTACT EMAIL]. Security reports: see /.well-known/security.txt on nexapair.ae.

This document is for information. The contract and its security schedule are what bind.