0REI Security Posture

Genesis v1.1

FIDUS AI – AN ASKEYCAPITAL COMPANY

0REI Security and Architecture Statement

Version: Genesis v1.1 **Date:** 2026-01-28

1. Data Custody

0REI is designed for self hosted deployment. Data residence and retention remain under Client control. No client data is sent to 0REI during normal operation.

2. Network and Telemetry

0REI does not require outbound internet access for runtime. The system is designed to run in isolated networks including air gapped environments. 0REI includes zero telemetry by default. No phone home behavior is required for operation.

3. Cryptography and Verification

- Signature algorithm: Ed25519
- Hash algorithm: SHA 256
- Canonicalization: RFC 8785 JSON Canonicalization Scheme (JCS)
- Binding: Collision resistant length prefixed binding root derivation
- Offline verification: Verifier tool validates signatures and binding roots without server access

4. Key Management

0REI does not persist private keys to disk. Keys are injected at runtime through environment variables or a Client chosen secret manager. Key custody is 100 percent Client owned.

5. Software Integrity and Builds

- Deterministic builds via Docker toolchains are recommended
- Images should be scanned for known vulnerabilities prior to deployment
- Rust implementation reduces memory safety risk classes

6. Supported Operating Environments

- Ubuntu 22.04 LTS x86_64
- Amazon Linux 2023

Other environments may work but are outside the supported scope for the pilot.

7. Security Questionnaire Note

For pilots, 0REI provides this standard posture statement. Full vendor security questionnaires are scoped to enterprise licensing and sized to the commercial opportunity.