SECURITY

Security whitepaper

How Keel stores, transmits, and protects your programme data. Written for IT security teams, procurement, and enterprise risk functions.

Executive summary

Keel is a TPM command centre that runs natively on the user's machine. In its default configuration, Keel stores all data locally in a SQLite database file and makes no network connections. There is nothing to approve at the firewall for a local-only installation.

When the optional sync feature is enabled by the user, all data is encrypted on the client device before transmission using AES-256-GCM with a key derived from the user's password. The Keel sync server receives and stores only ciphertext. Keel staff cannot read user data.

Data storage

Local-only mode (default)

By default, Keel operates without any network connectivity. All programme data — RAID log, decisions, actions, journal entries, people, documents — is stored in a single SQLite database file on the user's local filesystem.

- Database location (macOS): `~/Library/Application Support/keel/keel.sqlite`
- Database location (Linux): `~/.local/share/keel/keel.sqlite`

— Database location (Windows): `%APPDATA%\keel\keel.sqlite`

The database file is not encrypted at rest in local-only mode. Users who require encryption at rest should use their platform's full-disk encryption (FileVault, BitLocker, LUKS) which is the appropriate layer for this control.

Sync mode (optional, user-initiated)

When the user enables sync, Keel performs end-to-end encryption of all project data on the client device before any transmission occurs.

The encryption process:

- A 256-bit encryption key is derived from the user's password using Argon2id (m=65536, t=3, p=4)
- The user's email address is used as an additional salt to prevent cross-account attacks
- Project data is serialised to JSON and encrypted using AES-256-GCM
- A unique 12-byte random nonce is generated for each encryption operation
- Only the resulting ciphertext (nonce + tag + encrypted bytes) is transmitted to the server

The Keel sync server stores the ciphertext, timestamps, and user account metadata. It does not store or have access to encryption keys, plaintext data, or programme content of any kind.

PROPERTY	VALUE
Encryption algorithm	AES-256-GCM
Key derivation	Argon2id (m=65536, t=3, p=4)
Nonce	12 bytes, cryptographically random per operation
Authentication tag	128-bit GCM tag (authenticates both ciphertext and nonce)
Key length	256 bits
Transport	HTTPS / TLS 1.3
Server-side storage	Ciphertext only — no plaintext ever stored server-side

Network communications

Local-only mode

No network connections are made. Keel does not phone home, check for updates automatically, or transmit any data.

Sync mode

The following connections are made when sync is enabled:

- **sync.keelapp.io** — encrypted project data push/pull, authentication tokens
- All connections use HTTPS with TLS 1.3 minimum
- JWT bearer tokens used for authentication (24-hour access tokens, 30-day refresh tokens)

AI features (optional)

If the user configures Claude API integration, note content is transmitted to Anthropic's API for processing. This is governed by Anthropic's privacy policy and data processing agreement. Keel recommends reviewing Anthropic's enterprise data handling policies before enabling this feature in regulated environments.

Keel also supports fully offline AI via Ollama, which runs a local language model with no network connectivity. This is the recommended configuration for environments where data must not leave the device.

Authentication and access control

Local-only mode

No authentication is required. Access is controlled by the operating system's filesystem permissions on the database file.

Sync mode

- Passwords hashed using bcrypt (cost factor 12)
- JWT access tokens expire after 24 hours
- JWT refresh tokens expire after 30 days

- No password reset via email by default — users retain sole control of their encryption key
- Multi-device access requires the same password on each device (key derivation is deterministic)

Telemetry and analytics

Keel collects no telemetry, usage analytics, crash reports, or diagnostic data. There is no analytics SDK, no tracking pixel, and no background reporting.

The only network traffic from a Keel installation (beyond explicit sync or AI calls initiated by the user) is a version check on application startup, which transmits only the current application version number. This check can be disabled in Settings.

Data portability and deletion

Export

All data can be exported at any time as a complete JSON archive (Settings → Data → Export All Data). Individual entities (RAID, decisions, actions, people) can be exported as CSV files suitable for import into Excel or Google Sheets.

Deletion — local

Deleting the application database file removes all local data completely.

Deletion — sync server

Sync account deletion removes all server-side ciphertext within 30 days. Because the server stores only encrypted data, there is no plaintext to recover after deletion regardless.

Infrastructure (sync server)

COMPONENT	DETAIL

Backend	Go (Gin framework)
Database	PostgreSQL — stores ciphertext only
Hosting	Fly.io (EU region available on request)
TLS	1.3 minimum, managed by Fly.io edge
Backups	Daily automated PostgreSQL backups, 7-day retention
Access logging	Auth events and API call timestamps only — no content logged

Compliance and certifications

Keel is an independent product currently without formal certifications (ISO 27001, SOC 2, etc.). For enterprise deployments requiring certifications, the recommended configuration is local-only mode, which places the application entirely within your existing security perimeter and compliance controls.

The open data format (SQLite + JSON export) means programme data can be migrated to any compliant storage system without vendor lock-in.

Contact

Security questions, vulnerability disclosures, and enterprise security assessments: security@getkeel.com

Document version 1.0 · April 2026 · This document describes the security model of Keel v1.0. It is updated with each major release.

K

KEEL

TPM Command Centre

PRODUCT	LEGAL
Features	Privacy policy
Pricing	Terms of service
Download	Security