

Information Security Policy

Version 1.0 · Effective 1 November 2026 · Owner: Aleksandr Senkevich, katelabs, Belgrade, Serbia · katelabs.io

1. Purpose and scope

This policy sets out how katelabs protects the systems that collect, score, store and deliver its dataset, and the information clients share with it. It covers the collection pipeline, the database, the website and API, the delivery channels, and every device and account used to operate them. katelabs is operated by a single engineer; the controls below are sized for that reality and are written so that a reader can verify them.

2. Information classification

- **Public:** research notes, the open dataset slice, the website.
- **Licensed:** the full dataset, the index, API responses. Delivered only to authenticated licensees.
- **Confidential:** client contact details, contracts, usage logs, client feedback, anything a client marks confidential.
- **Secret:** credentials, API keys, signing keys, database connection strings, exchange keys.

Confidential and secret information is never placed in research notes, logs shared outside katelabs, or third-party AI tools.

3. Access control

1. Every account used to operate katelabs (cloud, database, code hosting, domain, email, exchange) has multi-factor authentication enabled.
2. Production credentials exist only in the hosting platform's secret store and in a password manager; they are not kept in source code, chat history or documents. The repository is scanned for committed secrets before each release.
3. Access is least-privilege: the collection process can write headlines; the website can only read; delivery keys can only read the data their licence covers.
4. Each licensee receives an individual API key or delivery credential. Keys are revoked on contract end or on request within one business day and can be rotated by the licensee at any time.
5. Any contractor or future employee receives access only to the systems their task requires, under a written confidentiality undertaking, and that access is removed when the task ends.

4. Encryption

All traffic to the website, the API and the database is encrypted in transit with TLS. The database and backups are encrypted at rest by the managed provider. Files delivered to licensees are transferred over authenticated HTTPS or a channel the licensee specifies; no data is sent by unencrypted email.

5. Infrastructure and change management

1. Services run on managed cloud platforms with provider-maintained operating systems; katelabs does not operate its own servers.
2. Code changes go through version control with a reviewable history. Dependencies are pinned and updated on a regular schedule; security advisories for dependencies are checked at least monthly and critical fixes are applied within seven days.
3. Production and development use separate databases and credentials. Production data is not copied to personal devices except as encrypted, access-controlled snapshots used for analysis, which are deleted when the analysis ends.

6. Logging and monitoring

Collection, scoring and delivery produce logs that record what ran, when, and with what result. Logs contain no credentials and no client confidential data. API access is logged per key. Failures in collection are detected automatically and surfaced to the operator; a gap in collection longer than one hour triggers an investigation.

7. Backups and continuity

The database is backed up continuously by the managed provider with point-in-time recovery, and a full export is taken at least weekly to a second, independent storage location. Restoration is tested at least twice a year. Because the dataset is append-only and every record carries its own timestamps, a restored database can be verified against delivered files. The target recovery time for delivery services is one business day.

8. Incident response

1. A security incident is any confirmed or suspected unauthorised access to systems, credentials or client information, or any corruption of the dataset.
2. On detection the operator contains the incident (revoking credentials, isolating the service), preserves logs, and records a timeline.
3. Affected licensees are notified within 72 hours of confirmation with what happened, what data was involved and what they should do. Where the law of a client's jurisdiction requires faster notice, that requirement prevails.
4. A written post-incident review is produced within two weeks and the resulting changes are tracked to completion.

9. Vendors

katelabs relies on a small number of vendors: cloud hosting, a managed database, code hosting, a language-model provider for scoring, and an email provider. Each is a major provider with published security certifications. Vendors receive only the data needed for their function; the language-model provider receives headline text and no client information. The vendor list is available to licensees on request.

10. Client responsibilities and review

Licensees are responsible for protecting the keys issued to them and for access within their own organisation. This policy is reviewed at least annually and after any incident. Questions and security reports: **aler.senkevich3301@gmail.com**; reports are acknowledged within two business days.