TRUST CENTER — SECURITY & COMPLIANCE

The security posture behind your search infrastructure

Every control we run to protect your data — encryption, access, network isolation, privacy and resilience — documented for your vendor security review.

DOCUMENT	LAST REVIEWED	REVIEW CYCLE	NEXT REVIEW
Security Overview	July 2026	Every 3 months	October 2026

A transparent view of how we protect your data. This document maps the security controls Opensolr operates to the five SOC 2 Trust Services Criteria and to the SIG / CAIQ vendor questionnaires, so your team can complete a vendor security review in one read. For our certified standards, see our ISO 9001 & ISO 27001 certification.

CONTROL SUMMARY

The one-page answer

The fastest response to most questionnaire rows. Each domain is expanded in the sections that follow.

DOMAIN	STATUS	DETAIL
Encryption in transit	✓ In place	TLS 1.2/1.3 only (1.0/1.1 refused), HSTS preload, HTTP→HTTPS enforced across site, API and every hosted index.
Encryption at rest	✓ In place	Account and identity data encrypted at rest on our primary data servers (AWS).
Authentication	✓ In place	Per-index HTTP Basic auth on every request, optional two-factor authentication, role-based access control.
Network isolation	✓ In place	Solr is never exposed to the public internet — bound to localhost behind authenticated Apache; default-deny firewalls fleet-wide.
Payment data	✓ None stored	No card or billing data on our servers; payments run through PCI-compliant Stripe.
Backups & recovery	✓ In place	Automated, transaction-consistent, off-site backups plus cross-region index replication.
Monitoring	✓ 24 / 7	Automated watchdog health checks with self-healing restarts; 99.9% uptime target.
Data privacy	✓ GDPR	Minimal data collection, documented privacy terms, right to erasure on request.
Framework alignment	✓ SOC 2 TSC	Controls mapped to the five SOC 2 Trust Services Criteria and the SIG / CAIQ vendor questionnaires.

TRUST SERVICES CRITERIA

Mapped to the five SOC 2 principles

CRITERION	HOW OPENSOLR ADDRESSES IT
Security	**Protected on every layer.** Authentication, IP rules, application firewall and network isolation stand between any request and your data.
Availability	**Built to stay up.** Redundant, replicated infrastructure with an automated watchdog that restarts failed nodes. 99.9% uptime target.
Confidentiality	**Your data stays yours.** Access is limited to the account owner and invited team members. Our staff never access index data without your consent.
Processing Integrity	**Complete & accurate.** Changes are made only by authorized users, with change logs and revision trails for a full audit history.
Privacy	**Minimal by design.** We collect only an email and a password. No selling, no sharing, and no payment data on our servers.

DATA PROTECTION

Encryption & access control

Encryption

- ✓ **In transit:** TLS 1.2/1.3 only; 1.0/1.1 refused. HSTS with a two-year preload policy and forced HTTPS.
- ✓ **Modern ciphers:** A+ grade cipher suites; certificates renewed on a regular annual cycle.
- ✓ **At rest:** account and identity data encrypted on our primary data servers (AWS).
- ✓ **Everywhere:** the same standard covers the website, the REST API and every hosted Opensolr Index.

Authentication & authorization

- ✓ **Per-index HTTP Basic auth** on every request — no anonymous access to your data.
- ✓ **IP access rules** per request handler: allow-list or block addresses, even with valid credentials.
- ✓ **Two-factor authentication** (Authy / SMS, via Twilio) available on every account.
- ✓ **Role-based access control** for team members; optional password lock on the public search page.

PLATFORM HARDENING

Application & infrastructure security

Application layer

- ✓ **Content Security Policy** and a full set of security headers applied centrally.
- ✓ **Parameterized database access** and search-query isolation to prevent injection.
- ✓ **Signed API requests:** destructive operations require an HMAC signature; keys never travel in a URL.
- ✓ **Rate limiting** per user and per IP, with automated abuse blocking and bot challenges.
- ✓ **CSRF protection & XSS filtering** platform-wide; cookies are Secure, HttpOnly and SameSite.

Network & infrastructure

- ✓ **Solr is never public.** Every node binds to localhost behind authenticated Apache — the only door is HTTPS with auth.
- ✓ **Default-deny firewalls** on every server; databases are not exposed to the internet.
- ✓ **Web application firewall** with bot, scanner and known-exploit filtering at the edge.
- ✓ **Hardened Solr:** data-import, config-editing and core-admin endpoints blocked; Log4Shell mitigated fleet-wide.
- ✓ **Segregated administration** through a jump host — production servers are not directly reachable.

PRIVACY & GDPR

Data privacy

Opensolr collects the **minimum data possible** — an email address and a password. We do not sell, trade or share personal information, and your Opensolr Index data is never accessed by our staff or subcontractors without consent, except in an urgent technical emergency required to restore service. **No card or billing data ever touches our servers** — all payments run through PCI-compliant Stripe. Full terms live in our GDPR Privacy Agreement and Privacy Policy.

AVAILABILITY & RESILIENCE

Backups, replication & uptime

Backups you control

- ✓ **Automated backups** that are transaction-consistent (no table locks) and copied off-site.
- ✓ **On-demand & scheduled index backups** — create, download or restore from the dashboard.

Resilience & monitoring

- ✓ **Cross-region index replication** for high availability and disaster recovery.
- ✓ **24/7 watchdog monitoring** that auto-restarts failed nodes; 99.9% uptime target.

VULNERABILITY & INCIDENT MANAGEMENT

How we stay ahead

- ✓ **Quarterly internal security testing.** We re-run our security review every three months and refresh this document with the results.
- ✓ **Proactive hardening.** We patch and mitigate emerging threats across the fleet — from framework CVEs to edge-level abuse — before they reach customers.
- ✓ **Documented incident handling.** Every critical change and incident is logged and revisioned for a full transparency trail.
- ✓ **Responsible disclosure.** Found something? Email support@opensolr.com and we'll respond promptly.

TRANSPARENCY

Sub-processors

The third parties that help us deliver the service, and what each one handles.

PROVIDER	PURPOSE	DATA HANDLED
AWS	Primary data servers & hosting	Account data, hosted indexes
Hetzner, HostHatch, Alibaba Cloud	Regional Solr hosting	Hosted index data (your region choice)
Stripe	Payments & billing (PCI-compliant)	Payment details — never stored by Opensolr
Twilio / Authy	Two-factor authentication delivery	Phone number, for 2FA only
Freshdesk	Support helpdesk	Support correspondence

STANDARDS & CERTIFICATIONS

Standards & certifications

Opensolr maintains **ISO 9001** (quality management) and **ISO 27001** (information security) certification. Our full Information Security Policy covers confidentiality, integrity, availability, authenticity and non-repudiation in depth.

Where your process calls for a SOC-style review, the controls documented here map directly to the SOC 2 Trust Services Criteria and to SIG / CAIQ questionnaires — enough for most vendor security assessments to proceed.

FOR ENTERPRISE REVIEWS

Available on request

- ✓ This Security Overview as a PDF.
- ✓ Completed SIG / CAIQ or custom security questionnaire responses.
- ✓ A Data Processing Agreement (DPA) for GDPR compliance.
- ✓ An architecture and data-flow overview for your risk assessment.

Contact **support@opensolr.com** or use the contact form at opensolr.com/contact.

REFERENCE DOCUMENTATION

Read the detail

Information Security Policy

Solr Cloud Data Security

Platform Security Guide

GDPR Privacy Agreement

Privacy Policy & Terms & Conditions

Opensolr SRL

VAT #: RO-35410526 · Cluj-Napoca, Romania · +40 737 883 303
opensolr.com · support@opensolr.com · https://opensolr.com/trust-center
Generated September 5, 2026 · Last reviewed July 2026 · Next review October 2026