TRi-Lo

Solutions

Programme intelligence for humanitarian infrastructure

Security Whitepaper

Programme Intelligence Platform for Humanitarian Infrastructure

TRi-Lo Solutions · trilosolutions.com · Mail@tri-lo.com

Document version 1.0 · Published May 2026 · Classification : Confidential

Contents

1. Executive Summary

TRi-Lo Solutions operates a multi-tenant Software-as-a-Service (SaaS) platform designed for the management of humanitarian and infrastructure development programmes. The platform serves organisations that manage donor-funded projects across multiple countries, often in challenging operational environments with limited connectivity.

Security is treated as a continuously-verified property of the system, not a point-in-time exercise. Every promise made in this document is backed by automated tests that run on every code change, and by public security audits that can be independently verified at any time.

Security highlights

- **Mozilla Observatory : A+ (125/100)** — 10/10 security tests passed
- **SSL Labs : A+ (Exceptional)** — 0 warnings, 2 endpoints
- **HSTS preloaded** — eligible for inclusion in Chrome / Firefox / Safari built-in preload list
- **Strict Content Security Policy** — no inline scripts, no unsafe-eval
- **19 automated Firestore security rules tests** — multi-tenant isolation, RBAC, audit logs immutability
- **22 end-to-end authenticated user-journey tests** on every commit
- **Daily multi-organisation data audit** — anomaly detection across 8 coherence zones
- **Automated CI/CD pipeline** — typecheck, lint, unit tests, rules tests, E2E tests, build verification on every push

Document scope

This whitepaper covers the security posture of the TRi-Lo Solutions SaaS platform available at **trilosolutions.com**. It is intended for prospective customers, partners, donors, and their information security teams. The document is updated quarterly. For the latest version, please contact **Mail@tri-lo.com**.

2. Platform Architecture

TRi-Lo Solutions is a modern web application built on cloud-native infrastructure managed by Google Cloud Platform (via Firebase) and Netlify. The architecture is deliberately serverless to minimise the attack surface and eliminate the need to operate and patch traditional server infrastructure.

Components

Frontend	React 18 + TypeScript single-page application, built with Vite. Distributed as a Progressive Web App (PWA) supporting offline operation.
Hosting & CDN	Netlify (global CDN with edge deployment, automatic HTTPS via Let's Encrypt, DDoS protection at the edge).
Authentication	Firebase Authentication (Google Cloud). Supports email/password with optional MFA, Google SSO, and token-based invitation flows.
Database	Cloud Firestore (Google Cloud). Document-based NoSQL with multi-region replication and per-document security rules enforced server-side.
File storage	Firebase Cloud Storage (Google Cloud). Encrypted at rest with AES-256.
Serverless functions	Netlify Functions (AWS Lambda underneath). Used for backend operations requiring privileged credentials.
Error monitoring	Sentry (EU region). Captures and aggregates application errors without storing personal data.
Source code	Private GitHub repository with branch protection, required CI checks, and signed commits.

Geographic data residency

Customer data is stored in Google Cloud regions selected for compliance with European data protection requirements. All sub-processors operate either in the European Union or under equivalent data protection frameworks (Standard Contractual Clauses, EU-US Data Privacy Framework).

3. Data Security

Encryption in transit

All connections to the platform use TLS 1.2 or higher. The TLS configuration is publicly graded **A+ (Exceptional)** by SSL Labs, with perfect forward secrecy and modern cipher suites only. HTTP connections are rejected at the edge and redirected to HTTPS. HTTP Strict Transport Security (HSTS) is enforced with a 2-year duration and is eligible for inclusion in the browser preload list.

Encryption at rest

All customer data is encrypted at rest using AES-256, the industry standard. Encryption keys are managed by Google Cloud Key Management Service (KMS) and rotated automatically. Backups are similarly encrypted.

Multi-tenant isolation

Each customer organisation operates within its own logically-isolated tenant. Isolation is enforced at the database layer through Firestore Security Rules — code that runs on every read and write operation, evaluated server-side and outside the application code path. A user authenticated to organisation A cannot, by design and by enforcement, access any data belonging to organisation B.

This isolation is verified by an automated test suite of **19 distinct security rules tests** running against the Firebase emulator on every commit. Tests cover cross-tenant reads, cross-tenant writes, role escalation attempts, and invitation token misuse. Any change to the security rules that would break isolation is rejected by the CI pipeline before deployment.

Audit logs

Every significant action within the platform (project create/update/delete, payment record changes, membership changes, etc.) is captured in a per-organisation audit log. Audit logs are **append-only by enforcement** — no user, including administrators, can modify or delete an audit record. This is verified by automated tests on every commit. Read access to audit logs is restricted to managers and administrators of the organisation.

Daily data integrity audit

An automated audit runs every morning at 7 AM and scans every customer organisation for data anomalies across 8 coherence zones: payment vs. project consistency, grouped procurement quotes, projects missing procurement plans, abnormal values (overpayments, negative figures, completion above 100%), workflow delays, date inconsistencies, ghost projects, and key performance indicator distribution. Anomalies are flagged immediately via macOS notification.

4. Access Control & Authentication

User authentication

User authentication is handled by Firebase Authentication, a hardened identity service operated by Google Cloud. Supported methods include email/password, Google SSO, and token-based invitations. Multi-factor authentication (MFA) is available and recommended for administrator accounts. Password hashing uses Google's internal implementation, which exceeds OWASP recommendations.

Role-based access control (RBAC)

Within each organisation, users are assigned one of four roles, each with explicitly enforced privileges:

Owner	Full administrative access. Cannot be removed by another administrator.
Admin	Full administrative access except organisation deletion.
Manager	Can create and update data. Cannot delete or change organisation settings.
Viewer	Read-only access. All write controls are hidden in the user interface and rejected server-side.

Invitation flow

New users are added to an organisation through a token-based invitation flow. The invitation token is bound to a specific email address at creation time. The platform verifies, server-side via security rules, that the email of the accepting user matches the invitation email before granting membership. This prevents interception of invitation tokens from being usable.

Internal access by TRi-Lo Solutions

TRi-Lo Solutions personnel do not have routine access to customer data. Privileged access (via Google Cloud service accounts) is restricted to a single named individual and is used only for specific support operations explicitly requested by the customer or for emergency data recovery. All privileged operations are logged and reviewable.

5. Application Security & Testing

Defence in depth

Application security is enforced through multiple independent layers, designed so that the failure of any single layer does not compromise the system:

- **TypeScript strict mode** — eliminates entire classes of runtime errors at compile time
- **Content Security Policy (CSP)** — strict, no unsafe-inline or unsafe-eval, blocking cross-site scripting at the browser level
- **Subresource Integrity (SRI)** — every external script verified by cryptographic hash before execution
- **Firestore Security Rules** — server-side enforcement of access controls, tested with 19 automated tests
- **Input validation** — all user inputs validated client-side and re-validated server-side
- **Honeypot anti-spam** — silent dropping of bot submissions on contact forms

Continuous integration pipeline

Every code change is validated by a continuous integration pipeline before being eligible for deployment. The pipeline runs three independent job categories in parallel:

Typecheck, lint, build	TypeScript compilation, ESLint analysis, unit tests (353 tests), production build verification.
Security rules tests	19 automated tests against the Firebase emulator, validating multi-tenant isolation and access controls.
End-to-end tests	22 Playwright tests simulating real user journeys: authentication, navigation, write operations, sign-out.

The same pipeline runs daily on a schedule, catching infrastructure-level regressions such as dependency updates breaking compatibility, certificates approaching expiry, or external service changes.

Dependency management

Application dependencies are pinned to specific versions and reviewed before upgrade. Automated security alerts from GitHub Dependabot flag known vulnerabilities in dependencies. Critical updates are applied within 7 days; non-critical updates are batched monthly.

6. Public Security Audits

Two independent, public, free-to-verify security audits continuously evaluate the platform's web security posture and TLS configuration. Anyone can re-run these audits at any time, providing transparent and verifiable evidence of the security controls described in this document.

Mozilla Observatory — A+ (125 / 100)

Mozilla Observatory evaluates the security headers and policies served by a web application. The platform scores **A+ with 125 out of 100** (a score above 100 reflects additional security headers beyond the standard requirements). All 10 tests are passed:

- Content Security Policy — strict, with SHA256 hash for inline SEO data
- Cookies — no insecure cookies
- Cross-Origin Resource Sharing — controlled exposure
- Redirection — HTTP forced to HTTPS
- Referrer Policy — strict-origin-when-cross-origin
- Strict Transport Security — 2 years, includeSubDomains, preload-eligible
- Subresource Integrity — all external scripts hash-verified
- X-Content-Type-Options — nosniff
- X-Frame-Options — DENY (clickjacking impossible)
- Cross-Origin-Resource-Policy & Cross-Origin-Opener-Policy — same-origin isolation

Verify : developer.mozilla.org/en-US/observatory/analyze?host=trilosolutions.com

SSL Labs (Qualys) — A+ (Exceptional)

SSL Labs by Qualys evaluates the Transport Layer Security (TLS) configuration of a domain, including protocol versions, cipher suites, certificate quality, and resistance to known attacks. The platform achieves the **A+ grade with the 'Exceptional' qualifier**, the highest classification awarded by SSL Labs, on all endpoints with zero warnings:

- TLS 1.3 supported, TLS 1.0 and 1.1 disabled
- Modern cipher suites only, perfect forward secrecy
- OCSP stapling enabled
- Certificate issued by Let's Encrypt, automatically renewed
- Resistant to known TLS attacks (Heartbleed, POODLE, BEAST, FREAK, etc.)

Verify : ssllabs.com/ssltest/analyze.html?d=trilosolutions.com

HSTS Preload — Pending Browser Inclusion

The domain has been submitted to the HSTS Preload list maintained by Chrome and consumed by Firefox, Safari, Edge, and other major browsers. Once propagated, browsers will refuse any HTTP connection to **trilosolutions.com** or any subdomain on the very first visit, eliminating SSL stripping attacks even against first-time visitors.

7. Compliance & Sub-processors

Current compliance posture

GDPR (EU 2016/679)	Compliant. Privacy policy published, data processing register maintained, Standard Contractual Clauses in place with sub-processors. Data subject rights (access, deletion, portability) supported via direct request to Mail@tri-lo.com.
Cyber Essentials (UK gov)	Application in preparation.
ISO 27001	Roadmap defined for certification within 12 months. Internal controls aligned with ISO 27001 Annex A in place.
SOC 2 Type I	Roadmap defined for completion following ISO 27001.

Sub-processors

The following sub-processors are used to deliver the service. All sub-processors are bound by Data Processing Agreements aligned with GDPR Article 28 and operate with mature, independently-certified security practices.

Google Cloud / Firebase	Authentication, database, file storage, cloud functions. ISO 27001, ISO 27017, ISO 27018, SOC 2 Type II, SOC 3 certified. EU region.
Netlify	Hosting, CDN, serverless functions, TLS termination. SOC 2 Type II certified.
Sentry	Error monitoring. SOC 2 Type II certified. EU region instance.
Let's Encrypt	TLS certificate issuance. ISRG (operator) is SOC 2 audited.
GitHub	Source code hosting. SOC 1 Type II, SOC 2 Type II, ISO 27001 certified.

8. Incident Response

Detection

Application-level incidents are detected through several independent channels:

- Sentry error monitoring — real-time aggregation of application exceptions
- Daily automated data integrity audit — scans all customer organisations for anomalies
- Netlify deploy monitoring — twice-daily check of build and deployment health
- Continuous integration pipeline — daily scheduled run catches infrastructure drift
- Customer reports via Mail@tri-lo.com

Response procedure

Upon detection of a security incident:

- **Within 1 hour** — initial assessment of scope and severity
- **Within 4 hours** — affected customers notified directly via email if any customer data may have been impacted
- **Within 24 hours** — initial root cause analysis
- **Within 72 hours** — formal incident report shared with affected customers (in compliance with GDPR Article 33 timeline for personal data breaches)
- **Post-incident** — remediation, regression test added to CI to prevent recurrence

Customer-facing communication

All security-related communications use a dedicated contact: **Mail@tri-lo.com**. Customers can reach this address at any time to report a suspected vulnerability, request a security review, or escalate an incident. Responsible disclosure of vulnerabilities is welcomed and acknowledged within 48 hours.

9. Business Continuity & Disaster Recovery

Backups

A complete export of all Firestore data is performed daily and retained for 60 days. Backups are encrypted at rest and stored in a separate Google Cloud project from production, with restricted access. A documented restore procedure is tested quarterly.

Recovery objectives

RTO (Recovery Time Objective)	4 hours for full service restoration after a disaster recovery scenario.
RPO (Recovery Point Objective)	Maximum 24 hours of data loss (daily backup cadence).
Availability target	99.5% measured monthly, with no formal SLA at present stage. Underlying providers (Google Cloud, Netlify) advertise 99.95–99.99% availability.

Offline operation

The platform is designed as a Progressive Web App with full offline support. Field users can continue viewing and recording data without internet connectivity for extended periods. Changes are synchronised automatically when connectivity is restored, with conflict resolution applied.

Vendor concentration

We acknowledge concentration risk on Google Cloud (Firebase) and Netlify. Migration paths to alternative providers have been identified for each critical component should a long-term outage occur. Source code, data exports, and customer-controlled configurations remain portable.

10. Verification & Contact

Independent verification

Every claim in this whitepaper that can be externally verified is verifiable today, by anyone, without contacting us :

Mozilla Observatory grade	developer.mozilla.org/en-US/observatory/analyze?host=trilosolutions.com
SSL Labs grade	ssllabs.com/ssltest/analyze.html?d=trilosolutions.com
HSTS preload status	hstspreload.org/?domain=trilosolutions.com
HTTP response headers	Use any HTTP inspection tool (curl, browser DevTools)
Public source visibility	JavaScript bundle is signed (Subresource Integrity) and verifiable

Documents available on request

- Data Processing Agreement (GDPR Article 28) — template available immediately
- CAIQ Lite questionnaire (Cloud Security Alliance v4) — pre-filled, sent on request
- Sub-processor list with their compliance certifications
- Detailed architecture diagram (under NDA)
- Security incident history (under NDA)

Contact

Security inquiries	Mail@tri-lo.com
Vulnerability disclosure	Mail@tri-lo.com — acknowledged within 48h
Customer support	Mail@tri-lo.com
Website	trilosolutions.com

This whitepaper is reviewed and updated quarterly. The current version is always available on request. Document version 1.0, published May 2026.