TESTRELIC AI — LEGAL

Security

Last updated: June 30, 2026

Security is foundational to how we build and operate TestRelic. This document summarizes our program and practices.

1. Data Protection

- Encryption in transit using TLS 1.3 and at rest using AES-256.
- Logical isolation of customer data within our multi-tenant architecture.
- We do not use Customer Data to train third-party foundation models.

2. Access Control

- Role-based access control (RBAC) for customer organizations.
- Least-privilege access for personnel, with access reviews.
- Authentication safeguards and audit logging for sensitive operations.

3. Infrastructure

The platform runs on hardened cloud infrastructure (AWS) with network controls, automated patching, and continuous monitoring. See our Sub-processors document for the providers we rely on.

4. Compliance Posture

We align our controls with the SOC 2 Type II framework and operate the platform to be GDPR-ready. Data processing terms are available in our Data Processing Agreement. We will share current compliance reports and certifications, where available, under NDA on request.

5. Resilience

- Automated backups and recovery procedures.
- Incident response procedures with defined severity levels and breach-notification commitments.
- Availability targets described in our Service Level Agreement.

6. Responsible Disclosure

If you believe you have found a security vulnerability, please report it to security@testrelic.ai. We ask that you give us a reasonable opportunity to remediate before public disclosure and that you avoid accessing or modifying

data that is not yours.

7. Contact

Security questions and reports: security@testrelic.ai