Security & Compliance Overview

This document provides an overview of the security practices, controls, and compliance posture followed by our URL Shortener Platform and Public APIs. It is intended for enterprise customers, partners, and security review teams.

Document Version: 1.0

Last Updated: February 2026

1. Product Overview

Our platform provides a secure, scalable URL shortening service with API-first architecture. Customers can programmatically generate short URLs, manage redirections, and access analytics using authenticated REST APIs over HTTPS.

2. Security Architecture

• API-first design with no anonymous write access
• All API traffic encrypted using HTTPS (TLS 1.2+)
• Token-based authentication for all protected endpoints
• Logical separation between public APIs and internal systems

3. Authentication & Access Control

• API access protected using secure API keys / tokens
• Tokens are scoped and revocable
• Unauthorized access attempts are blocked and logged
• No hard-coded credentials in application code

4. Data Protection

• No sensitive personal or health data is required for core URL shortening functionality
• Data in transit is encrypted using industry-standard TLS
• Input validation enforced to prevent injection attacks
• Error responses are sanitized to avoid information leakage
• Application data is stored securely on cloud infrastructure with controlled access.

5. API Security Controls

• Rate limiting and throttling enabled to prevent abuse
• Protection against common API attacks (OWASP API Top 10)
• Validation of request headers, payloads, and parameters
• Monitoring for anomalous usage patterns

6. Vulnerability Management & VAPT

• Regular Vulnerability Assessment & Penetration Testing (VAPT)
• Testing aligned with OWASP API Security Top 10 guidelines
• Findings classified by severity (Critical, High, Medium, Low)
• Timely remediation of identified risks and retesting where required

We are currently in the process of conducting a Vulnerability Assessment & Penetration Testing (VAPT) assessment for our public APIs. The VAPT certificate will be shared upon completion, if required.

7. Logging & Monitoring

• Centralized logging of API access and security events
• Monitoring for failed authentication attempts and abnormal traffic
• Logs retained for operational and security analysis

8. Compliance Statement

Our security controls and processes are designed to meet the expectations of enterprise customers in regulated sectors such as healthcare, finance, and technology. The platform follows industry best practices for application and API security.

9. Security Contact

For security-related questions, assessments, or disclosures, please contact:
Email: contact@insprl.com
Response Time: 1–2 business days