Information Security Summary

Effective Date: 01/01/2026

This Information Security Summary describes the measures implemented by Reliable Insights Ltd ("Reliable Insights") to protect the confidentiality, integrity, and availability of information processed through the Reliable Insights Platform and associated services.

1. Information Security Governance

Reliable Insights maintains an information security framework appropriate to the size, nature, and risk profile of the organisation and the Services provided.

Security responsibilities are assigned to senior management, and information security is reviewed periodically as part of operational and risk management activities.

2. Risk Management

Reliable Insights applies a risk-based approach to information security, including:

- identification of information security risks
- proportionate controls based on likelihood and impact
- periodic review of risks and mitigations

This approach is aligned with recognised standards, including ISO/IEC 27001 principles.

3. Access Control

Access to systems and data is controlled through:

- role-based access controls
- least-privilege principles
- individual user authentication
- timely removal of access upon role change or departure

Administrative access is restricted to authorised personnel only.

4. Data Security

Reliable Insights implements appropriate technical and organisational measures to protect data, including:

- segregation of customer environments
- encryption of data in transit where appropriate

- secure storage of credentials and secrets
- controlled handling of backups and logs

Customer data is processed solely in accordance with contractual agreements and documented instructions.

5. Network and Infrastructure Security

Security controls are applied across infrastructure and network layers, including:

- firewalls and network segmentation
- monitoring for unauthorised access
- secure configuration and patch management
- restricted administrative interfaces

Third-party hosting providers are selected based on security and reliability criteria.

6. Secure Development Practices

Reliable Insights applies secure development practices, including:

- separation of development, test, and production environments
- access controls on source code repositories
- review and testing prior to deployment
- controlled release and change management

7. Incident Management

Reliable Insights maintains incident response procedures designed to:

- detect and assess security incidents
- contain and mitigate impact
- notify affected customers where required
- comply with applicable data protection obligations

Personal data breaches are reported in accordance with UK GDPR requirements.

8. Business Continuity and Resilience

Measures are in place to support service continuity, including:

- data backup and recovery procedures
- redundancy within hosted environments where appropriate

- documented recovery processes

Business continuity arrangements are proportionate to service criticality.

9. Supplier and Third-Party Security

Third-party suppliers and sub-processors are assessed for security risk where they have access to systems or data.

Appropriate contractual protections are in place to ensure confidentiality and data protection obligations are met.

10. Personnel Security and Awareness

Reliable Insights ensures that:

- staff are subject to confidentiality obligations
- access is granted based on role and necessity
- security awareness forms part of onboarding and ongoing practices

11. Compliance and Review

Reliable Insights monitors compliance with its information security policies and reviews controls periodically.

This Information Security Summary may be updated from time to time to reflect changes in risk, services, or regulatory requirements.

12. Contact

For information security enquiries, please contact:

Reliable Insights Ltd
Email: security@reliable-insights.com
Website: https://reliable-insights.com