Data Security Policy

Information Security & Data Protection Standards

Document Version	2.1
Effective Date	March 2026
Last Reviewed	March 15, 2026
Classification	Public
Owner	Spry Insights FZCO

Spry Insights FZCO | Dubai, UAE
Contact: security@spryinsights.com

Table of Contents

1. Executive Summary

AIRA Analytics, developed by Spry Insights FZCO, is committed to maintaining the highest standards of data security and privacy. This policy outlines the technical and organizational measures we implement to protect client data throughout its lifecycle.

Our security framework is designed to meet the requirements of enterprise clients, including multinational corporations with stringent data protection standards. We employ industry-standard encryption, access controls, and monitoring to ensure data confidentiality, integrity, and availability.

Key Security Commitments:

- All data encrypted in transit (TLS 1.3) and at rest (AES-256)
- No client data used for AI model training
- Data stored in SOC 2 Type II certified infrastructure
- Complete data deletion within 30 days of contract termination
- Regular third-party security assessments

2. Scope & Applicability

This policy applies to all data processed through the AIRA Analytics platform, including:

- Survey response data uploaded by clients
- Analysis outputs and reports generated by the platform
- User account information and access credentials
- System logs and usage analytics
- Any derivative data created during analysis

3. Data Classification

AIRA Analytics classifies data into the following categories, with corresponding security controls:

Classification	Description	Security Controls
Confidential	Client survey data, PII, analysis outputs	Encryption, access logging, MFA required
Internal	System configurations, user accounts	Role-based access, audit trails
Public	Marketing materials, public documentation	Standard web security

4. Infrastructure Security

4.1 Cloud Infrastructure

AIRA Analytics is hosted on enterprise-grade cloud infrastructure with the following certifications:

Certification	Status	Scope
SOC 2 Type II	Active	Infrastructure provider
ISO 27001	Active	Infrastructure provider
GDPR Compliant	Active	Data processing operations
CSA STAR	Active	Cloud security controls

4.2 Network Security

- Web Application Firewall (WAF) with real-time threat detection
- DDoS protection with automatic mitigation
- Network segmentation isolating client data environments
- Intrusion Detection System (IDS) with 24/7 monitoring
- Regular vulnerability scanning and penetration testing

5. Data Encryption

5.1 Encryption Standards

Data State	Encryption Method	Key Management
In Transit	TLS 1.3 (minimum TLS 1.2)	Automated certificate rotation
At Rest	AES-256-GCM	Hardware Security Module (HSM)
In Processing	Memory encryption	Ephemeral keys
Backups	AES-256 with separate keys	Geographically distributed

5.2 Key Management

Encryption keys are managed through a dedicated Key Management Service (KMS) with the following controls:

- Keys stored in FIPS 140-2 Level 3 validated HSMs
- Automatic key rotation every 90 days

- Separate keys per client environment
- Key access logged and audited

6. Access Control

6.1 Authentication

- Multi-Factor Authentication (MFA) required for all users
- Single Sign-On (SSO) integration available (SAML 2.0, OAuth 2.0)
- Password requirements: minimum 12 characters, complexity enforced
- Session timeout after 30 minutes of inactivity
- Failed login lockout after 5 attempts

6.2 Authorization

AIRA implements Role-Based Access Control (RBAC) with the following standard roles:

Role	Permissions	Typical Assignment
Admin	Full platform access, user management	Client IT administrators
Analyst	Upload data, run analysis, view reports	Research team members
Viewer	View reports only	Stakeholders, executives
API User	Programmatic access only	Integration systems

7. Data Processing & Storage

7.1 Data Isolation

Each client's data is logically isolated through:

- Dedicated database schemas per client
- Unique encryption keys per client
- Network-level isolation between client environments
- No cross-client data access possible at application level

7.2 AI Processing

Important: Client data is never used to train AI models. All AI processing is performed using:

- Pre-trained foundation models (no fine-tuning on client data)
- Stateless processing — no data retained after analysis completion
- Isolated processing environments per analysis job
- Outputs are generated fresh for each request

8. Incident Response

Spry Insights maintains a documented Incident Response Plan with defined procedures for security events. Key commitments include:

Incident Type	Initial Response	Client Notification
Critical (data breach)	Within 1 hour	Within 24 hours
High (attempted breach)	Within 4 hours	Within 48 hours
Medium (vulnerability)	Within 24 hours	In monthly report
Low (policy violation)	Within 72 hours	As needed

In the event of a confirmed data breach affecting client data, we will provide:

- Immediate notification to affected clients
- Detailed incident report within 72 hours
- Root cause analysis and remediation plan
- Support for client's regulatory notification requirements

9. Compliance & Certifications

AIRA Analytics is designed to support client compliance with major data protection regulations:

Regulation	Applicability	Key Features
GDPR	EU data subjects	DPA available, data portability, right to deletion
CCPA	California residents	Data access requests, opt-out support
PDPA	Singapore	Consent management, data protection
DPDP Act	India	Data localization options, consent framework

10. Data Retention & Deletion

10.1 Retention Periods

Data Type	Retention Period	Deletion Method
Uploaded survey data	Duration of contract + 30 days	Cryptographic erasure
Analysis outputs	Duration of contract + 30 days	Cryptographic erasure
Access logs	12 months	Automated purge
Backups	90 days rolling	Secure overwrite

10.2 Data Deletion

Upon contract termination or client request, data deletion follows this process:

- Client notified 30 days before scheduled deletion
- Option to export all data before deletion
- Cryptographic key destruction renders data unrecoverable
- Certificate of destruction provided upon request
- Backup copies purged within 90 days

11. Third-Party Security

AIRA Analytics uses a limited number of vetted third-party services. All third parties are:

- Subject to security assessment before engagement
- Bound by data processing agreements
- Required to maintain SOC 2 or equivalent certification
- Reviewed annually for continued compliance

12. Contact Information

For security-related inquiries or to report a security concern:

Security Team	security@spryinsights.com
Data Protection Officer	dpo@spryinsights.com
General Inquiries	hello@spryinsights.com

— End of Document —

This document is subject to change. The latest version is always available upon request.