WISE ATHENA

WISEATHENA · PUBLIC SUMMARY

# Information Security Overview

Version 1.0 · 2026

| | |
|---|---|
| **Document** | Information Security Overview |
| **Audience** | Clients, prospects and partners |
| **Owner** | Information Security Officer (ISO) |
| **Review frequency** | At least annually |
| **Contact** | security@wiseathena.com |

## 1. About This Document

This document provides a high-level overview of WiseAthena's Information Security programme. It is intended for external audiences — clients, prospects and partners — who wish to understand our approach to protecting information assets.

WiseAthena is a B2B technology company specialising in data analytics and processing services. Protecting the confidentiality, integrity and availability of information entrusted to us by our clients is a core operational commitment.

## 2. Security Commitment

WiseAthena's Information Security programme is built on three foundational principles:

| | |
|---|---|
| **Confidentiality** | Sensitive information assets are accessible only to duly authorised individuals and systems. |
| **Integrity** | Information assets are safeguarded against unauthorised modification or destruction. |
| **Availability** | Authorised users have timely and reliable access to information assets. |

## 3. Governance & Organisation

Information security governance at WiseAthena operates across multiple levels of the organisation:

| ROLE | RESPONSIBILITY |
|---|---|
| Board of Directors | Oversight, strategic direction and accountability for the security programme |
| Risk Committee | Supervises risk management strategy, security governance and policy review |

| ROLE | RESPONSIBILITY |
|---|---|
| Chief Operations Officer | Establishes and maintains the information security programme; leads strategy and oversight |
| Information Security Officer (ISO) | Leads day-to-day security operations: policies, risk management, incident response and awareness |
| All employees & contractors | Responsible for adhering to security policies and reporting incidents and anomalies |

Security performance indicators (KPIs) are reported to the Board of Directors at least annually. Key Risk Indicators (KRIs) are reported at least quarterly.

## 4. Scope of the Security Programme

The Information Security programme applies to all employees, contractors, consultants and any third party accessing WiseAthena's information assets or IT resources. It covers:

- All IT resources and systems, both on-premise and cloud-based
- All information and data assets transmitted or stored on company-owned resources
- Any device connected to company networks or used to access company IT resources
- Cloud services and third parties that process or store information assets on behalf of the organisation

## 5. Security Policies & Controls

The programme is governed by a comprehensive, documented and reviewed policy framework. The areas covered include, but are not limited to:

| | |
|---|---|
| Incident Response | Access Control |
| Data Asset Management | Third-Party Vendor Management |
| Encryption | Network Security |
| Security Training & Awareness | Remote Access |
| Asset Management | Change Management |
| Configuration & Hardening | BYOD Security |
| Business Continuity & DR | Patch Management |
| Secure Development | Antivirus & Antimalware |
| Password Management | Acceptable Use |
| Vulnerability Management | Penetration Testing |

## 6. Key Security Controls

### Access Management

Access to information assets is granted based on the principle of least privilege and is reviewed periodically. Remote access requires multi-factor authentication (MFA) with a minimum of two factors, and all remote connections are secured with appropriate encryption.

### Risk Management

Information security risks are identified, documented and managed throughout the lifecycle of IT resources. Risks are recorded in a formal Risk Register and escalated to the Risk Committee when they exceed the organisation's defined risk appetite.

### Incident Management

A formal Incident Response Policy governs the detection, reporting, handling and mitigation of security incidents. Security events and anomalous activities are monitored and analysed in a timely manner. All personnel are required to report security incidents immediately to security@wiseathena.com.

### Business Continuity

Business Continuity and Disaster Recovery plans are developed, maintained and tested at least annually to ensure operational resilience in the event of a disruption.

### Vendor Management

Third-party services that process or store information on behalf of the organisation are subject to security oversight, periodic review and compliance validation.

### Compliance

Information assets are managed in accordance with all applicable laws, regulations and industry standards. The security programme is reviewed at least annually, and following any significant regulatory change.

## 7. SOC 2 Alignment

WiseAthena is currently undergoing a SOC 2 audit aligned to the Security Trust Services Criteria (CC series). Our programme has been designed to satisfy the following control categories:

- **CC1 — Control Environment:** governance structure, accountability and ethical commitment
- **CC2 — Communication & Information:** security policy dissemination and reporting
- **CC3 — Risk Assessment:** formal risk identification and treatment
- **CC4 — Monitoring Activities:** continuous monitoring and regular reviews
- **CC5 — Control Activities:** technical and procedural controls across systems and processes
- **CC6 — Logical & Physical Access:** access management, MFA and encryption
- **CC7 — System Operations:** incident detection, response and recovery
- **CC8 — Change Management:** formal change control processes
- **CC9 — Risk Mitigation:** vendor management and business continuity

## 8. Contact

For questions about WiseAthena's Information Security programme, please contact:

| | |
|---|---|
| Security enquiries | security@wiseathena.com |

Exceptions to security policies require formal documentation and approval in accordance with the organisation's Policy Management Procedures.