



## **A.I.M ENTERPRISE GROUP (PTY) LTD**

# Data Handling & Information Security Policy

---

### **PUBLIC PRODUCTION VERSION**

Innovate • Integrate • Elevate

EFFECTIVE 18 AUGUST 2026 | LAST UPDATED 2 OCTOBER 2026

Applies to A.I.M Enterprise Group, AIM One and supporting technology services.

This public policy describes how A.I.M Enterprise Group handles and protects information across AIM One and supporting technology services. It is intended to reflect the current production platform at the date above and should be read with our Privacy Policy, Terms & Conditions and any applicable customer agreement.

## 1. Purpose and Scope

A.I.M Enterprise Group (Pty) Ltd ("A.I.M Enterprise Group", "A.I.M", "we", "us" or "our") is committed to protecting information entrusted to our businesses, products and technology platforms.

This Data Handling & Information Security Policy explains how we handle, protect and manage information processed through A.I.M Enterprise Group systems, with particular focus on AIM One, our internal customer relationship workflows and connected services.

This policy should be read together with our Privacy Policy, Terms & Conditions and any applicable product, service, subscription or customer agreement.

## 2. Technology Platform and Service Providers

AIM One is operated using a combination of cloud infrastructure and third-party technology services. These services support authentication, data storage, application hosting, transactional email, integrations and communications.

| AREA                              | DESCRIPTION                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Supabase                          | Database, authentication, backend services and secure data access for AIM One and related internal systems.                                    |
| Netlify                           | Hosting and delivery of the AIM One web application and other A.I.M web interfaces.                                                            |
| Resend                            | Transactional email delivery, including invitations, account confirmations, password resets and other service-related messages.                |
| Meta / WhatsApp Business Platform | Optional WhatsApp Business onboarding, messaging, webhook events and related account or phone-number integrations where enabled by a customer. |
| Other approved providers          | Monitoring, analytics, support, communications, security or operational services where reasonably required.                                    |

### NOTE

AIM One does not depend on every external service for every function. A failure of one integration should, where reasonably possible, affect only the relevant feature rather than the entire platform.

## 3. AIM One and Customer Data

AIM One is a modular business operating system designed to help organisations manage their own business information and workflows.

Information entered into AIM One by a customer remains associated with that customer's organisation account. A.I.M Enterprise Group does not treat one customer's operational database as a general marketing database for unrelated purposes.

- Customer and contact information
- Leads, opportunities and sales activity
- Quotes and invoices
- Finance and accounting records
- Projects, tasks and jobs
- Inventory and advanced inventory information
- Point-of-sale information
- Rental and booking information
- HR and workforce information
- Customer Operations activity, attribution and interaction history
- Integration data and external activity events
- Other operational information entered or generated through enabled AIM One modules

## 4. A.I.M Enterprise Group's Role

A.I.M Enterprise Group develops, provides and operates AIM One and the supporting infrastructure required for the platform to function. Our role may include platform administration, maintenance, security, technical support, reliability, product improvement and incident response.

The business using AIM One remains responsible for the information it collects and enters into the platform and for ensuring its own use of personal information complies with applicable law, contractual obligations and industry requirements.

## 5. Customer Responsibilities

Businesses using AIM One are responsible for appropriate and lawful use of the information they manage through the platform.

- Collecting and using information lawfully
- Providing notices and obtaining consent where required
- Keeping information accurate where appropriate
- Managing user access within their organisation
- Using WhatsApp and other integrations in accordance with applicable platform rules and law
- Responding to lawful requests from their customers concerning personal information
- Removing or correcting information when reasonably required
- Protecting their own account credentials, devices and user access

## 6. Tenant-Based Data Separation

AIM One uses a tenant-based model. Each business is associated with its own organisation account and information is scoped to that organisation.

Customer information belonging to one AIM One organisation should not ordinarily be available to another unrelated AIM One organisation merely because both use the same platform.

Tenant separation is supported by database-level controls, application permissions and organisation-scoped access logic. These controls are reviewed and improved as the platform develops.

### NOTE

Example: information belonging to Business A should not be visible to Business B unless there is a legitimate, authorised and technically permitted relationship between those records or users.

## 7. Users, Roles and Permission Controls

AIM One restricts access according to organisation membership, enabled modules, role and permission scope. Not every user receives the same access.

| AREA                           | DESCRIPTION                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Platform Administrator         | Authorised A.I.M technical or administrative access used for platform operation, maintenance and support.                |
| Business Owner / Administrator | Broad access to their own organisation and its enabled modules.                                                          |
| Manager / Staff                | Access limited to assigned business responsibilities and configured permissions.                                         |
| Read-only / limited roles      | View access without modification where configured.                                                                       |
| Support / technical access     | Restricted access used only where reasonably necessary to resolve an authorised support, reliability or security matter. |

## 8. Authentication and Account Security

Authentication is provided through Supabase Auth and related AIM One account controls. Users are expected to protect their credentials and use accounts assigned to them rather than sharing passwords.

AIM One may use email confirmation, password reset, invitation workflows, multi-factor authentication or other account-security features depending on configuration and product availability.

- Passwords and authentication credentials should not be shared.
- Users should report suspected unauthorised access promptly.
- Organisation administrators should remove or restrict access when a user no longer requires it.
- Security-related notifications may be sent when account details or authentication methods change.

## 9. Privileged and Server-Side Access

Certain backend functions require privileged server-side access that is not made available directly to ordinary browser users.

Where AIM One uses elevated service credentials for protected backend routes, those routes are expected to perform the relevant authentication, tenant and permission checks before accessing privileged data.

Direct browser access to sensitive integration tables is restricted where those records are intended to be handled through secured server-side application routes.

**NOTE**

Privileged credentials are treated as secrets and should never be exposed in browser code, customer-visible screens, public repositories, screenshots or support messages.

## 10. Customer Operations, External Activity and Attribution

AIM One Customer Operations can combine customer records with manual activity, AIM One system events and events received from approved external systems.

External activity sources may use API credentials and external identity mappings so that events can be associated with the correct AIM One contact or company.

- External customer or user identifiers
- Activity types and event timestamps
- External references used for duplicate protection
- Source-system identifiers
- Attribution information such as source, campaign or conversion context where provided
- Technical metadata required to process, match, secure or troubleshoot an event

**NOTE**

Where an event cannot be safely matched to a customer, it may remain unmatched rather than being attached to an incorrect record.

## 11. Integration Security and Duplicate Protection

External integrations are expected to authenticate using valid credentials issued or approved for the relevant connection. Invalid or unauthorised requests may be rejected.

AIM One uses external references and database constraints in relevant integration workflows to reduce duplicate event creation when the same external event is received more than once.

Integration configuration, audit receipts and operational status information may be retained where reasonably necessary for security, troubleshooting and reliable processing.

## 12. WhatsApp Business Platform and Meta

Where WhatsApp functionality is enabled, AIM One is designed so that each customer organisation connects and uses its own WhatsApp Business account and WhatsApp Business phone number rather than sharing a single common AIM One number.

AIM One may process information necessary to operate the connection, including WhatsApp Business Account identifiers, business phone number identifiers, customer or contact identifiers, message content where required for the requested functionality, message status information, timestamps, templates, webhook events and related technical metadata.

Meta and WhatsApp separately process information under their own terms, policies and platform requirements. AIM One customers remain responsible for lawful and compliant use of WhatsApp through their organisation account.

## 13. Transactional Email and Resend

AIM One uses transactional email for account and service-related communications such as invitations, email confirmations, password resets and security notifications.

Resend is used as an email-delivery provider for these communications. Email addresses, message-routing information and technical delivery metadata may be processed as necessary to deliver and troubleshoot these messages.

Transactional account emails are separate from optional marketing communications.

## 14. Security Measures

A.I.M Enterprise Group takes reasonable technical and organisational measures to protect information against unauthorised access, loss, misuse, alteration, disclosure or destruction. Security controls vary according to the system, feature and risk involved.

- Authentication controls through Supabase Auth
- Tenant- and role-scoped application permissions
- Database-level access controls, including Row Level Security where applicable
- Protected server-side routes for privileged operations
- HTTPS/TLS for web communications
- Restricted handling of service credentials and integration secrets
- Logging and operational diagnostics where appropriate
- Backups and recovery capabilities provided by infrastructure services
- Security updates, maintenance and dependency management

- Permission checks for sensitive administrative and integration functions

## 15. Credentials, API Keys and Secrets

API keys, access tokens, service credentials and other secrets are treated as sensitive authentication information.

Users and administrators must not place credentials in customer notes, screenshots, public documents, chat messages, source repositories or other locations where they may be exposed.

A.I.M Enterprise Group may rotate, revoke or replace integration credentials where reasonably necessary for security, operational or customer-support purposes.

## 16. Data Stored With Third-Party Providers

AIM One depends on third-party cloud services to provide parts of its infrastructure and integrations. These providers may process or store information in jurisdictions outside South Africa.

Where providers process information on our behalf, A.I.M Enterprise Group aims to select and configure services with appropriate security and privacy capabilities and to take reasonable steps to address applicable cross-border processing requirements.

Third-party services may experience outages, maintenance events, policy changes or security incidents outside A.I.M Enterprise Group's direct control.

## 17. Backups and Recovery

AIM One may use backup and recovery mechanisms provided by its infrastructure services to protect against accidental loss, system failure or other technical incidents.

Backup copies may temporarily contain information that has been deleted from the active system until the relevant backup cycle expires or is replaced in accordance with provider and operational retention practices.

Recovery capabilities reduce risk but do not constitute a guarantee that every item of data can always be restored in every circumstance.

## 18. Monitoring, Logging and Audit Records

AIM One may retain technical logs, integration receipts, security events, timestamps and other operational records where reasonably necessary to operate, troubleshoot, secure or audit platform activity.

Logging is intended to support reliability and accountability while avoiding unnecessary exposure of sensitive customer content. Additional audit controls may be introduced as platform requirements evolve.

## 19. Security Incidents and Data Breaches

If A.I.M Enterprise Group becomes aware of a security incident involving unauthorised access to, loss of or disclosure of personal information, we will assess the incident and take reasonable steps appropriate to the circumstances.

- Contain and investigate the incident
- Protect affected systems and credentials
- Determine what information may have been affected
- Take corrective or recovery action
- Document relevant findings where appropriate
- Comply with applicable legal and regulatory obligations
- Notify affected parties or regulatory authorities where required by law

## 20. Data Retention, Export and Account Closure

Information is retained for as long as reasonably necessary to provide services, maintain accounts, support business operations, comply with legal or regulatory obligations, resolve disputes, maintain financial or security records and protect legitimate business interests.

Retention periods differ according to the type of information, the customer relationship, enabled modules and applicable requirements. AIM One does not apply one automatic deletion period to every category of data.

Where supported by the relevant AIM One service, customers may export or retrieve information associated with their organisation account. When an account is closed, information may be deleted, anonymised or retained for a limited period where reasonably necessary for legal, accounting, security, recovery or dispute-resolution purposes.

## 21. Confidentiality and Use of Customer Data

Information stored within AIM One may contain confidential business information. Authorised A.I.M personnel, contractors and service providers who legitimately encounter such information are expected to handle it responsibly and confidentially.

A.I.M Enterprise Group does not use one AIM One customer's customer database as a general source of contacts for unrelated A.I.M marketing merely because the information is stored within the platform.

Access to customer data by A.I.M personnel should be limited to legitimate platform, support, security, operational or legal purposes.

## 22. Analytics and Platform Improvement

A.I.M Enterprise Group may use technical, diagnostic or aggregated information to monitor performance, identify errors, improve security, understand system usage and develop future features.

Where reasonably possible, information used for broad analytical or development purposes should be aggregated, anonymised or minimised so that individual customer records are not unnecessarily exposed.

## 23. Access Requests and Data Rights

Where personal information is stored within AIM One on behalf of a customer organisation, requests concerning that information will generally need to be handled by the organisation that collected and controls the relevant customer relationship.

A.I.M Enterprise Group may provide reasonable technical assistance where appropriate and where required by law or the applicable service arrangement.

Requests relating directly to information controlled by A.I.M Enterprise Group can be sent to [admin@aimenterprisegroup.co.za](mailto:admin@aimenterprisegroup.co.za). Sufficient information should be provided to allow us to identify the relevant account, organisation or records.

### NOTE

Example: if a customer of Business A requests access to information that Business A stores in AIM One, Business A remains responsible for handling that request, while A.I.M may assist with the technical aspects where appropriate.

## 24. Continuous Improvement and Policy Updates

AIM One is an evolving technology platform. Security, privacy, permissions, logging, integration controls and administrative safeguards may be strengthened or changed as the platform grows and risk requirements evolve.

We may update this policy to reflect changes to AIM One, our infrastructure, integrations, security practices, laws or data-handling processes. The latest public version will be published through A.I.M Enterprise Group's website or other appropriate customer channel.

## 25. Contact

Questions regarding this policy, AIM One data handling, security practices or privacy-related technical requests can be directed to A.I.M Enterprise Group.

| AREA    | DESCRIPTION                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Company | A.I.M Enterprise Group (Pty) Ltd                                                                                                                                     |
| Email   | <a href="mailto:admin@aimenterprisegroup.co.za">admin@aimenterprisegroup.co.za</a>                                                                                   |
| Website | <a href="https://www.aimenterprisegroup.co.za/">https://www.aimenterprisegroup.co.za/</a>                                                                            |
| Address | A.I.M Enterprise Group operates as a digital-first business. Services are delivered remotely or on-site where applicable; we do not maintain public-facing premises. |