A.I.M ENTERPRISE GROUP (PTY) LTD

Data Handling & Information Security Policy

REVISED DRAFT

Innovate • Integrate • Elevate

EFFECTIVE 18 AUGUST 2026 | LAST UPDATED 18 AUGUST 2026

Prepared for internal review and pre-launch customer onboarding.
Recommended for formal legal review once budget allows.

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 A.I.M Enterprise Group approaches the handling and protection of information, particularly information stored within **A.I.M ONE** and processed through our internal customer relationship management system ("CRM").

This policy should be read together with our **Privacy Policy** and applicable service-specific agreements.

1. Our Technology Platform

INFRASTRUCTURE

A.I.M Enterprise Group's technology is built on the following infrastructure:

- **Supabase** — provides the database, authentication and backend infrastructure for A.I.M ONE and A.I.M's internal CRM. All customer and business data is stored here.
- **Netlify** — hosts the front-end applications (including the CRM interface and, where applicable, parts of A.I.M ONE) that customers and staff interact with in the browser.

Netlify is primarily a hosting layer for the application interface. Supabase is where information is actually stored, secured and processed. This policy is written with that architecture in mind.

2. A.I.M ONE and Customer Data

A.I.M ONE is a technology product of A.I.M Enterprise Group.

A.I.M ONE is designed to provide businesses with tools to manage their own business operations and information, which may include:

- Customer information
- Leads
- Bookings
- Jobs
- Projects
- Inventory
- Rentals
- Point-of-sale information
- Business records
- Internal operational information
- Other information entered by the business

Information entered into A.I.M ONE by a customer remains associated with that customer's business account.

A.I.M Enterprise Group does **not** treat the operational information stored by a business within A.I.M ONE as its own general customer database.

3. A.I.M's Role

A.I.M Enterprise Group provides and operates the A.I.M ONE platform, the internal CRM, and the infrastructure required for these systems to function. Our role may include:

- Providing the software platform
- Maintaining the platform and its Supabase-based infrastructure
- Improving platform functionality
- Providing technical support
- Monitoring platform performance and security
- Protecting the platform from misuse
- Maintaining system reliability
- Addressing technical or security incidents

The business using A.I.M ONE remains responsible for the information it enters into the platform and for ensuring that its collection and use of personal information complies with applicable laws.

4. Access to Customer Data

A.I.M Enterprise Group does not use customer business data stored within A.I.M ONE as a general resource for its own unrelated purposes.

However, A.I.M Enterprise Group — including its administrators and technical staff — may access customer information stored within A.I.M ONE or the internal CRM where reasonably necessary to:

- Provide technical support
- Diagnose or resolve a technical problem

- Maintain or improve the security of the platform
- Investigate suspected security incidents
- Prevent misuse or unauthorised activity
- Maintain or restore system functionality
- Perform necessary maintenance or development work
- Comply with a lawful legal or regulatory requirement
- Protect the rights, safety or security of A.I.M, its customers or the platform

Where access is necessary, A.I.M Enterprise Group will seek to limit access to the information reasonably required for the relevant purpose, and to authorised personnel only.

5. Customer Responsibility

Businesses using A.I.M ONE are responsible for the information they enter into the platform. This includes responsibility for:

- Collecting information lawfully
- Informing their customers where required
- Obtaining consent where legally required
- Keeping information accurate where appropriate
- Using information only for lawful purposes
- Managing their own customer relationships
- Providing appropriate access to their staff or authorised users
- Removing information when it is no longer required
- Responding to lawful requests from their customers concerning personal information

A.I.M ONE provides the technology and infrastructure that allows businesses to manage their information. It does not replace the business's own legal responsibilities.

6. Separation of Business Data

A.I.M ONE is built around a tenant-based model: every business using A.I.M ONE has its own organisation account, and business data is scoped to that organisation at the database level.

Customer information belonging to one A.I.M ONE business should not be made available to another unrelated A.I.M ONE business merely because both businesses use the A.I.M ONE platform.

> **EXAMPLE**
> Information belonging to **Business A** should not ordinarily be accessible to **Business B** unless there is an authorised reason and appropriate access has been established.

This separation is enforced through access controls at the database level (rather than relying only on the application interface) and is an important part of the platform's approach to protecting customer information. As A.I.M ONE develops, we will continue to strengthen and test these controls.

7. Internal Access Controls and Roles

Access to A.I.M systems and infrastructure is restricted according to legitimate business and technical requirements. Depending on the system, roles may include:

ROLE	ACCESS LEVEL
Platform Administrator	A.I.M technical/admin role with the broadest access, reserved for authorised A.I.M personnel
Business Owner	Full access to their own organisation's A.I.M ONE data
Manager / Staff	Access scoped to their role within a business's account
Read-only	Can view permitted information without modifying it
Support	Restricted technical access granted only where needed to resolve a specific issue

Where administrative or technical access is required, A.I.M Enterprise Group aims to:

- Limit access to authorised personnel
- Use appropriate authentication controls
- Restrict access according to role and responsibility
- Avoid granting more access than is needed for the task at hand
- Maintain appropriate system security controls
- Review access where reasonably necessary

A.I.M Enterprise Group will continue to improve these controls, including audit logging of sensitive administrative actions, as A.I.M ONE and its supporting infrastructure develop.

8. Security Measures

A.I.M Enterprise Group takes reasonable technical and organisational measures to protect information against unauthorised access, loss, misuse,

alteration or destruction. Depending on the system and service involved, these measures may include:

- Authentication controls (via Supabase Auth)
- Role-based and organisation-scoped access controls
- Database-level access controls (e.g. Row Level Security policies)
- Secure application architecture
- Encryption where appropriate
- Secure communications (HTTPS/TLS)
- Infrastructure security provided by our hosting and database providers
- Backups and recovery mechanisms
- Monitoring and logging
- Security updates
- Technical maintenance

Security measures may change as our technology and security requirements evolve.

9. Data Stored With Third-Party Infrastructure Providers

A.I.M ONE and A.I.M's internal CRM rely on the following third-party infrastructure and technology providers to operate:

- **Supabase** — database hosting, authentication and backend infrastructure
- **Netlify** — application/front-end hosting

We may also rely on other third-party providers for services such as email, communications, monitoring and security as needed.

Where third-party providers are used, A.I.M Enterprise Group aims to select services that provide appropriate security and privacy capabilities and to configure those services responsibly.

Some providers may process or store information outside South Africa. Where applicable, A.I.M Enterprise Group will take reasonable steps to address applicable legal requirements relating to cross-border processing.

10. Backups and Recovery

A.I.M ONE and our CRM may use backups and other recovery mechanisms provided through Supabase to protect against accidental loss, system failure or other technical incidents.

Backup copies may contain information that was present in the platform at the time the backup was created. Where information is deleted from the active system, copies may remain temporarily within backups until those backups are replaced or securely deleted in accordance with applicable retention practices.

11. Data Breaches and Security Incidents

A.I.M Enterprise Group takes security incidents seriously. If we become aware of an incident involving unauthorised access to or disclosure of personal information, we will assess the incident and take reasonable steps to:

- Contain the incident
- Investigate what occurred
- Protect affected systems
- Determine what information may have been affected
- Take corrective action
- Comply with applicable legal obligations
- Notify affected parties or regulatory authorities where required by law

The specific response will depend on the nature and seriousness of the incident.

12. Data Retention

A.I.M Enterprise Group retains information for as long as reasonably necessary to provide and operate its services, maintain customer accounts, support business operations, comply with legal and regulatory obligations, resolve disputes, maintain appropriate business records, protect the security of its systems, and fulfil other legitimate purposes.

Retention periods therefore vary depending on the nature of the information, the relationship with the customer, the services being provided and applicable legal requirements.

A.I.M Enterprise Group does not apply a single automatic deletion period to all information stored within its systems. Where information is no longer reasonably required, A.I.M may delete, anonymise, archive or otherwise dispose of it in accordance with applicable requirements and its operational procedures. As a general guide:

- **Active account** — data is retained while the account/service relationship exists.
- **Inactive account** — data may continue to be retained where there is a legitimate business, contractual, accounting, legal, security or operational reason.
- **Terminated account** — data is not necessarily immediately destroyed; A.I.M will determine what information needs to be retained and what can eventually be deleted or anonymised.

Certain information may be retained for longer periods where there is a legitimate business, legal, accounting, security, dispute-resolution or other lawful reason to do so.

13. Data Export and Account Closure

Where supported by the applicable A.I.M ONE service and subject to the relevant service terms, customers may be able to export or retrieve information associated with their account.

When an A.I.M ONE account is closed, information may be deleted, anonymised or retained for a limited period where reasonably necessary for:

- Legal compliance
- Financial or accounting requirements
- Security
- Dispute resolution
- Backup and recovery
- Protection of legitimate business interests

Specific deletion and export procedures may depend on the version and functionality of A.I.M ONE available at the time.

14. Confidentiality

A.I.M Enterprise Group recognises that information stored within A.I.M ONE may contain confidential business information. We expect authorised personnel, contractors and service providers who may legitimately encounter such information to handle it responsibly and confidentially.

Customer information should not be accessed, disclosed or used for purposes unrelated to legitimate platform, support, security or legal requirements.

15. Use of Customer Data by A.I.M

A.I.M Enterprise Group does not use customer business data stored within A.I.M ONE as a general source of customer information for unrelated marketing or commercial purposes.

In particular, A.I.M does not intend to use one A.I.M ONE customer's own customer database to market services to those individuals simply because their information is stored within the platform.

Any separate marketing relationship between A.I.M Enterprise Group and a business or individual will be handled in accordance with our Privacy Policy and applicable law.

16. Analytics and Platform Improvement

A.I.M may collect technical or aggregated information about how its platforms operate in order to monitor performance, identify errors, improve functionality, understand system usage, improve security and develop future features.

Where possible, information used for analytical or development purposes should be aggregated, anonymised or otherwise minimised so that individual customers are not unnecessarily identified. A.I.M Enterprise Group does not need to inspect individual customer records simply to understand overall platform performance.

17. Access Requests and Data Rights

Where personal information is stored within A.I.M ONE on behalf of a business's own customers, requests relating to that information will generally need to be handled by the business that collected and controls the relevant customer relationship.

> **EXAMPLE**
> If a customer of **Business A** requests access to information that Business A stores in A.I.M ONE, Business A remains responsible for responding to that request in accordance with applicable law.

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

18. Protection of A.I.M's Own Information

This policy also applies to information belonging directly to A.I.M Enterprise Group and its businesses, including customer, lead, supplier, employee/contractor, financial, website enquiry and communication records. Such information is handled in accordance with our Privacy Policy and applicable legal requirements.

19. Continuous Improvement

A.I.M ONE is a developing technology platform. As the platform grows, we intend to introduce additional security, privacy and data-management controls, including improvements to access management, authentication, audit logging, data separation, backup management, data export, account deletion and administrative controls.

Our policies and technical practices will therefore evolve as the platform develops, and this document will be updated accordingly.

20. Policy Updates

We may update this Data Handling & Information Security Policy when necessary to reflect changes to A.I.M ONE, our technology infrastructure, our security practices, applicable laws, or how information is processed. The latest version will be published on the A.I.M Enterprise Group website.

21. Contact

Questions regarding this policy or the handling of information within A.I.M platforms can be directed to:

Company	A.I.M Enterprise Group (Pty) Ltd
Email	info@aimenterprisegroup.co.za
Website	A.I.M Enterprise Group website
Address	A.I.M Enterprise Group operates as a digital-first business. Services are delivered remotely or on-site (where applicable, e.g. A.I.M Fabrication) — we do not maintain public-facing premises.

IMPORTANT NOTICE

This policy describes A.I.M Enterprise Group's actual and intended approach to handling information within its technology platforms, including A.I.M ONE (built on Supabase) and its internal CRM (hosted on Netlify). It is suitable for onboarding early customers but should be reviewed and formally adopted by a qualified South African privacy/legal professional as A.I.M ONE scales, particularly once tenant-level access controls, audit logging and a formal internal data governance policy are fully implemented.