

# PRIVACY POLICY STATEMENT

## Privacy Statement

At iAM Omni, we provide asset management software and related services to organisations worldwide. Protecting the privacy and security of corporate, personal, and client information is integral to our operations. This Privacy Policy explains how we collect, use, protect, and share information, and it reflects our commitment to align with ISO 27001:2022 Information Security Management System (ISMS) standards and relevant privacy regulations (e.g., Australian Privacy Principles, GDPR).

## Scope

This Privacy Policy applies to all iAM Omni operations, products, services, and online resources. It encompasses any information collected from current and prospective customers, employees, and other stakeholders.

## Our Commitment to Information Security

We are fully committed to aligning our operations with the ISO 27001:2022 Information Security Management System (ISMS) standards. This international framework guides our approach to risk management, data protection, and continuous improvement, ensuring that your information is managed with the highest level of care and security.

Our Privacy Policy Statement is our guide to ensuring the confidentiality of all information related to iAM Omni, our clients, and our employees. We believe our success comes from upholding this commitment in everything we do.

## Data We Collect

- **Identity & Contact Information:** Names, email addresses, phone numbers, and other relevant details necessary for account setup or communication.
- **Usage & Technical Information:** Analytics data (e.g., log files, IP addresses, device information, software usage patterns) to improve product functionality and user experience.
- **Client & Asset Data:** Data about client-owned assets and associated records maintained within our software, including metadata, asset configurations, performance, maintenance activities or location.
- **Minimal Personnel Data:** (where applicable): Basic human resources information (e.g., name, position, and limited contact details) used solely for recruitment, administration, or internal HR purposes.
- **Supplier & Partner Data:** Business contact and contract-related information (e.g., company name, representative names, addresses, and payment details) for managing supplier or partner relationships, procuring goods/services, and fulfilling legal or financial obligations.

## How We Use Your Data

### Service Delivery & Improvement

- **Client & Asset Data:** We use information about client-owned assets and associated records to provide, maintain, and enhance our software and services. This includes troubleshooting, customer support, and performance analytics aimed at continuously improving our offerings.
- **Usage & Technical Information:** Data such as log files, IP addresses, and software usage patterns help us optimize platform stability, identify and fix technical issues, and develop new features that improve user experience.

### Communication

- **Identity & Contact Information:** We rely on collected names, email addresses, or phone numbers to send service updates, respond to inquiries, and notify you of product developments or relevant offers—always in compliance with applicable communications laws.
- **Supplier & Partner Data:** We utilize business contact details to coordinate project timelines, manage invoices or contracts, and communicate necessary updates or information related to procurement and partnership agreements.

### Compliance & Legal Obligations

- **Personnel Data:** Limited HR or employment-related details are processed as needed for payroll, tax, or other legal mandates.
- **Client & Asset Data / Supplier & Partner Data:** We may need to process, retain, or disclose certain records to comply with contractual commitments, industry regulations, or statutory requirements. This includes adhering to financial auditing standards, government reporting obligations, or court orders.

### Security & Risk Management

- **All Data Categories:** We perform ongoing risk assessments, employ access controls, and utilize security analytics to protect our systems, detect fraud, and prevent unauthorized access. This may include evaluating network logs or usage metrics to identify suspicious activity and proactively mitigate potential threats.

### Supplier & Partner Engagement

- **Supplier & Partner Data:** We collect and use company details, representative information, and contract-related records to manage supplier or partner relationships effectively. Activities include contract negotiation, payment processing, performance review, and compliance with legal or contractual obligations.

## Personnel Administration

- **Personnel Data:** For internal HR purposes—such as recruitment, training, and employment administration—we collect and process only the minimum data needed. This may include contact details, payroll information, and performance reviews, all managed in line with confidentiality and retention requirements.

## Data Retention & Disposal

We retain and dispose of each category of data (Personnel, Client & Asset, Supplier & Partner) in accordance with documented retention schedules, which reflect contractual, legal, and regulatory obligations. Once the relevant retention period has passed or the data is no longer required, we securely delete or anonymize it following our disposal procedures.

### Personnel Data

**Scope:** Personal information related to employees or contractors (e.g., HR records, payroll details).

**Retention Period:** Retained only as long as necessary for employment, legal, or regulatory obligations. Once no longer needed, data is securely archived or deleted in accordance with our disposal procedures.

### Client & Asset Data

**Scope:** Asset-related data and other information gathered or generated through our software or services.

### Retention Period:

- **Contractual Alignment:** Stored for the duration of the client contract and any agreed-upon transition period afterward.
- **Regulatory Alignment:** Extended retention may apply where specific industry or legal mandates exist.

**Secure Disposal:** Data is securely deleted or anonymized once no longer needed for service delivery or compliance.

## 3. Supplier & Partner Data

**Scope:** Business contact information, contracts, invoices, payment details and other relevant documents for suppliers and partners.

### Retention Period:

- **Contractual & Financial Records:** Retained for as long as required to fulfill the terms of procurement, partnership agreements, or financial record-keeping requirements (e.g., for auditing or tax compliance).
- **Legal & Regulatory Alignment:** Where laws mandate specific durations for document retention (e.g., accounting or tax regulations), we adhere to those requirements.

**Secure Disposal:** Upon contract termination or expiration of mandatory retention periods, we securely remove or archive supplier data in line with our disposal procedures.

## Data Protection and Security

We apply robust systems, policies, and technical controls to protect all information from unauthorised access, disclosure, or misuse. Our ISMS framework ensures regular audits, risk assessments, access controls, and ongoing training for our staff to maintain compliance and security readiness.

## Employee Responsibility

All employees of iAM Omni are required to complete information security training and formally acknowledge all relevant company policies and procedures. Each individual understands that a duty of care is owed and agrees not to disclose or use any company information or intellectual property—including but not limited to company policies, procedures, employee details, and client information—except for the benefit of iAM Omni.

This culture of responsibility and accountability ensures that all data is managed with integrity and discretion.

## Your Choices & Rights

You may have the right to access, correct, or request deletion of certain personal data depending on the jurisdiction. For more information on how to exercise your choices and rights, please refer to the Contact Us section of our Privacy Policy.

## Contact Us

If you have any questions regarding our privacy practices or our information security management commitments, please contact us at: info@iamomni.com.au