

Information Security Policy Statement

The Senior Leadership team at Immij recognises the importance of protecting the organisation's information and information systems from both deliberate and accidental threats. An Information Security Management System (ISMS) is established and maintained in accordance with ISO 27001:2022 to ensure a structured, risk-based approach to protecting information and related assets.

Immij is committed to safeguarding the confidentiality, integrity and availability of information across all business activities, including information relating to customers, employees, suppliers and operations. This applies to information in all forms, including digital, physical and verbal.

Information security is a shared responsibility. All employees, contractors and relevant third parties are expected to:

- Protect information from unauthorised access, disclosure, alteration or loss
- Follow all information security policies, procedures and work instructions
- Use company systems and information appropriately and securely
- Ensure only approved suppliers and third parties are engaged in accordance with company requirements
- Only share information with external parties where authorised and appropriate controls are in place
- Exercise care when interacting with external parties, including verifying requests and remaining alert to suspicious activity
- Report information security incidents, weaknesses or concerns promptly
- Complete required information security training and maintain awareness of their responsibilities

Failure to comply with these requirements may result in disciplinary action.

Information security risks are identified and managed through a structured risk assessment process, with appropriate and proportionate controls implemented including those relating to suppliers and third-party service providers. Information security objectives are established and reviewed to support this policy and the strategic direction of the business.

Immij is committed to meeting applicable legal, regulatory and contractual information security requirements and maintaining the trust of customers and stakeholders.

The Senior Leadership team ensures that adequate resources, roles and responsibilities are in place to support the ISMS. The system is monitored, reviewed and continually improved to remain effective and responsive to changes in the business and evolving security risks.

This policy is communicated to all personnel as part of induction and ongoing training and is available to relevant external interested parties upon request.



Mark Randles | Group General Manager
May 2026