omni
talent is everything

Omni RMS
Information Security Policy Statement

OMNI – PS004

V5 2025 {Public}

Information Security Policy Statement

Omni RMS ("Omni") is committed to protecting all its information against any loss of confidentiality, integrity, and availability that could impact our finances, operations, legal or contractual obligations, or reputation. As part of this commitment, Omni will implement, maintain, and continually improve an ISO 27001-compliant Information Security Management System (ISMS) to enhance information security and cybersecurity resilience.

It is Omni's policy to:

- Protect all Omni's information assets against loss of confidentiality, integrity, or availability.
- Mitigate the risks associated with the theft, loss, misuse, damage, or abuse of these assets, including emerging cyber threats and technological advancements.
- Ensure that information users are aware of and comply with all current and relevant information security regulations and legislation.
- Provide a safe and secure information system working environment for employees and any other authorised users.
- Promote awareness and provide ongoing training for employees and authorised users to protect against social engineering, phishing, and other security threats.
- Implement and maintain cybersecurity resilience measures, including secure software development and the adoption of industry best practices.
- Make certain that all authorised users understand and comply with this policy and supporting policies and procedures.
- Protect the organisation from liability or damage through the misuse of its information.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the information they handle.

Omni will assess and regularly review all information security risks through Omni's risk assessment process, considering business objectives and external and internal factors, and define the necessary controls to mitigate these risks. Omni aims to stay ahead of changes in the profile and sophistication of threats and strives to implement controls that are fit for the future and not just immediate threats.

Omni will define information security objectives and improvement actions related to this policy and its information security risks. Omni will regularly evaluate progress against these objectives through the 'Management Review' process to ensure the business continuously improves its information security stance and goes beyond minimum legal requirements.

Omni will monitor access to and use of its information systems to establish the effectiveness of its ISMS, assess security measures, and identify potential improvements. This includes monitoring compliance with security protocols and reviewing the performance of technical and organisational controls.

Any employee or other authorised user who suspects a breach of information security must immediately inform a member of management. In the event of a suspected or actual security breach, Omni may disable or remove any users, data, or other elements necessary to secure its information systems.

This policy applies to all employees, visitors, contractors, and any other parties accessing Omni information. It covers the use of all Omni information assets, privately owned systems connected directly or indirectly to Omni's information systems, and all owned and/or licensed software and data.

Any failure to comply with this policy may lead to disciplinary action, including dismissal or prosecution. In the case of a contractor failing to comply, their contract may be cancelled, and the contractor may be reported to the relevant authorities, including the police.

Signed

Louise Shaw

Managing Director **Date: 6th February 2025**

omni

talent is everything

www.omnirms.com