



# Information Security Policy Statement

OMNI-PS004  
December 2021 v3

Omni Resource  
Management Solutions Ltd

## Information Security Policy Statement

Omni is committed to protecting all its information against any loss of confidentiality, integrity and availability that could impact on our finances, operations, legal or contractual obligations or on its reputation. As part of this commitment, Omni will implement, maintain and continually improve an ISO 27001 compliant information security management system.

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.
- 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.
- 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 and define the necessary controls to mitigate these risks. Omni aims to keep abreast 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 that are related to this policy and to its information security risks. Omni will regularly evaluate progress against these objectives through Omni's '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 in order to establish the effectiveness of its information management system and to identify potential improvements.

Any employee or other authorised user that suspects there has been or is likely to be a breach of information security has a duty to 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 anything else necessary to secure its information systems.

This policy applies to all employees, visitors, contractors and any other parties accessing Omni information. This policy relates to the use of all Omni information assets, to all privately owned systems when connected directly or indirectly to Omni's information systems and to all owned and/or licensed software/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 with this policy, their contract may be cancelled and the contractor reported to the relevant authorities, including the police.

Signed:

Date: 1<sup>st</sup> December 2021



Managing Director