Information Security Policy Statement

OMNI-PS004
August 2018 v1

Omni Resource Management Solutions Ltd

Information Security Policy Statement

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

It is our policy to:-

- Protect all our 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 staff 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.

We will assess and regularly review all information security risks through our risk assessment process and we will define the necessary controls to mitigate these risks.

We will define information security objectives and improvement actions that are related to this policy and to our information security risks. We will regularly evaluate progress against these objectives through our 'Management Review' process.

We will monitor access to and use of our information in order to establish the effectiveness of our information management system and to identify potential improvements.

Any staff 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, we may disable or remove any users, data or anything else necessary to secure our information systems.

This policy applies to all employees, visitors, contractors and any other parties accessing our information. This policy relates to the use of all our information assets, to all privately owned systems when connected directly or indirectly to our 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.