MRM Worldwide (UK) Ltd
Information Security Policy Statement

It is MRM's policy to develop, implement and maintain an Information Security Management System (ISMS) with the following strategic objectives:

1. Provide assurance within the company and to our customers, suppliers, partners, interested parties and other relevant stakeholders that the availability, integrity, and confidentiality of their information will be maintained appropriately, and that the organisation will drive continuous improvement of its ISMS;

2. Manage information security risks to all company and customer assets;

3. Protect the company's ongoing ability to meet contractual commitments through appropriate Business Continuity;

4. Base information security decisions and investments on risk assessment of relevant assets considering integrity, availability, and confidentiality;

5. Take into account business and legal or regulatory requirements, and contractual security obligations;

6. Maintain awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities;

7. Minimise the likelihood, business impact of, and deal effectively with, security incidents.

Responsibility for implementing this policy lies with the Managing Director. This policy will be reviewed annually to ensure that it continues to reflect the operations of the company and that it continues to comply with the requirements of ISO 27001.

This Policy is supported by the following operational objectives:

- Implementation and continuous improvement of an Information Security Management System that is fully compliant and independently certified to the ISO 27001 Standard for Information Security Management Systems.
- Implementation of information security policies including compliance with legal regulations including the General Data Protection Regulation (GDPR) (EU) 2016/679 to protect partner, supplier and employee information which is not in the public domain.

- Implementation of an Information Security Risk Assessment Procedure that assesses the harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and controls currently implemented.
- Development and implementation of a Business Continuity/Disaster Recovery Plan to counteract interruptions to the activities of MRM and to protect critical processes from the effects of major failures or disasters.
- Defined security-controlled perimeters and access-controlled offices and facilities to prevent unauthorised access, damage and interference to premises and information.
- Information Security Awareness guidance for all employees.
- An information security forum that supports the continuous review and improvement of the ISMS.
- Implementation of Incident Management and Escalation procedures for reporting and investigation of security incidents for ISMS management review and action.

To support achievement of these objectives, key performance indicators (KPIs) are set and maintained by the Process Director and reviewed quarterly with the Information Security Forum team. The record of these KPIs includes a reference to the applicable strategic and operational objectives above.

The company information security policy is reviewed by the Managing Director who recommends amendments and updates to the policy as part of the continuous service improvement process.

This Policy will be made available to interested parties, if relevant and appropriate.

Gareth Osborne

Gareth Osborne, Managing Director