# SECURITY POLICY

1.1 The Directors and Senior Management of IMServ share an agreed and declared commitment to this security policy. Accreditation to ISO 27001 is viewed as an objective measure of IMServ's commitment to providing a quality service to customers and complements IMServ's industry accreditations.

1.2 Information Security in IMServ means:

- The preservation of the availability, confidentiality and integrity of all physical and electronic information assets
- The protection of authorised access to information assets by agreed means and the prevention of unauthorised access to such assets via IMServ resources or by IMServ personnel
- The protection of the confidentiality, and integrity of content of such assets whilst under IMServ's control, during processing, or whilst on IMServ's premises
- The secure onward transmission of information assets to clients
- The preservation of client confidentiality
- The physical security measures necessary to protect information assets
- Continuous awareness, alertness, and vigilance by all staff in respect of security

1.3 IMServ's objectives are:

- To maintain the ISO 27001 accreditation (so as to maintain the confidence of customers (and others) in our ability to achieve the intended outcome)
- To protect all information assets
- To comply with contractual obligations for security and confidentiality
- To comply with legal obligations
- To comply with the requirements of the energy sector
- To comply with the requirements of the Smart Energy Code, specifically Sections G and I
- To improve awareness of all staff of the security controls and ISO 27001 requirements
- To promote continuous improvement of controls and standards (i.e via responding to security incidents, incident management, maintaining risk registers, audit results, penetration test results)

1.4 All employees of IMServ are expected to comply with this Security Policy. All staff will receive an appropriate level of education and training.

1.5 The Statement of Applicability identifies how information-related risks are controlled. Full compliance with all legislative and contractual requirements, development, testing and maintenance of a full business continuity plan and documented and published security incident reporting procedure are fundamental to this Policy.

1.6 This Security Policy is subject to continuous, systematic review and improvement to ensure that it remains aligned with IMServ goals and in order to reduce information related risks to the business to acceptable levels.

1.7 IMServ is committed to the independent assessment and approval of its security policy and management system via a third party Certification Body.

This policy may be amended by IMServ at any time but shall be routinely reviewed no less than once in any twelve month period.

Managing Director
Steve Brown