INFORMATION SECURITY POLICY

1 POLICY

It is the Company's policy to develop, implement and maintain an Information Security Management System that:

- Provides assurance within the company and to our clients and partners that the availability, integrity and confidentiality of their information will be maintained appropriately.
- Manages information security risks to all company and customer assets.
- Protects the company's ongoing ability to meet contracted commitments through appropriate Business Continuity.
- Bases information security decisions and investments on risk assessment of relevant assets considering; Integrity, Availability and Confidentiality.
- Takes into account business and legal or regulatory requirements, and contractual security obligations.
- Maintains awareness of all employees so they can identify and fulfil contractual, legislative and company specific security management responsibilities.
- Minimises the business impact and deals effectively with security incidents.
- Supports the company strategies though the OKR scheme for Information Security

This Policy is supported by the following objectives:

- Maintenance of a company wide Information Security Management System that is fully compliant and independently certified to the ISO/IEC 27001 Standard for Information Security Management Systems.
- Implementation of a sensitive information control policy including compliance with regulations under the Data Protection Act 1998 to protect client, partner, supplier, our own and personal employee information which is not in the public domain.
- Implementation of an Information Security Risk Assessment Process that assesses the business 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 Plan to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
- Defined security controlled perimeters and access to controlled offices and facilities to prevent unauthorised access, damage and interference to business premises and information.
- Information security awareness guidance for all company employees.
- An Executive Management Team that supports the continuous review and improvement of the company IMS.
- Implementation of incident management and escalation procedures for reporting and investigation of security incidents for IMS management review and action.

The company information security policy is reviewed by the Executive Management Team who recommends amendments and updates to the policy as part of the continuous service improvement process. The requirements of the Company's IMS are mandatory and all company personnel have a responsibility and obligation to its integrity. In the event of non-compliance with this policy, appropriate disciplinary action may be taken.