Information Security Management System Policy

STL Management has established an Information Security Policy, which supports the strategic aims of the business and is committed to maintaining and improving information security within STL and minimising its exposure to risks. It is therefore STL policy to:

- Ensure the confidentiality of corporate and client information
- Protect sensitive information (however stored) against unauthorised access
- Maintain the integrity of all information
- Ensure the availability of information, as required
- Provide information security training for all staff
- Ensure that the expectations and requirements of all interested parties, in relation to Information Security, are met
- Make information available to authorised business processes and employees when required
- Meet all regulatory/legislative requirements (Data Protection Act, Companies Act and Copyright law)
- Produce business continuity plans for business activities that are regularly maintained and tested
- Ensure that all breaches of information security, actual or suspected, will be reported to and investigated by STL and opportunities for improvement will be identified and acted upon
- Comply with the requirements of ISO 27001 for information security; and
- Communicate this policy statement to the public, through our website and on request

The policy is dynamic and includes a commitment to continual improvement through a process of incident reporting, risk assessment and regular audits. It complements the established ISO9001 and ISO14001 Management Systems and provides a framework for establishing and reviewing security objectives. STL Management is responsible for communicating the company's Information Security Policy and making sure it is understood at all levels.

The policy is subject to annual review when it is amended as necessary to ensure it remains appropriate.

STL Communications Limited
October 2017