Security Policy

S2S is committed to safeguarding the confidentiality, integrity and availability of all physical and electronic information assets of the organisation and its customers to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security are;

- Develop, Implement and review policies and processes
- Ensure compliance with current laws, regulations and guidelines
- Identify and review all risks and impacts of breaches and develop objectives for risk reduction
- Comply with requirements for confidentiality, integrity and availability for S2S's stakeholders
- Establish controls for protecting information and information systems against theft, abuse and other forms of harm and loss
- Provide a safe and secure environment for client's equipment and information using a layered approach to both physical and digital information security
- Ensure the availability and reliability of the network infrastructure and the services supplied by S2S
- Ensure confidentiality of data
- Ensure that S2S is capable of continuing their services even if an incident occurred
- Work with employees to maintain the responsibility for, ownership of and knowledge of information security such that the risk of security incidents is reduced
- Communicate all polices and working instructions to Customers, Employees and all other interested parties
- Continually improve the information security system

The directors and all employees are committed to an effective Information Security Management System in accordance with its strategic business objectives.

S2S's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information-related risks through establishing and maintaining this policy.

It has been decided that information security is to be ensured by this policy, management systems and a set of working instructions. In order to secure operations at S2S even after a serious incident, S2S shall ensure the availability of continuity plans, back up procedures, defence against malicious activities, system and information access controls, physical security, staff vetting, incident management and reporting.

Failure to comply with this or any other relevant policy or work instructions may lead to disciplinary actions for staff or contract restrictions and cancellations for suppliers and third parties.

The information security objectives will be reviewed on an annual basis and are based on the risk assessments and company objectives.

Version Control Table

Version	Date	Author	Status	Description of Change
1.0	06/06/19	David Smith	Draft	Template created from WI template, to be used for new Policy Documents
1.1	06/06/19	David Smith	Live	Update wording on objectives after copied from previous policy
1.2	09/09/19	David Smith	Live	Updated to reflect layered security approach
Approved Date: 09/09/2019				
Approved By: David Smith				
Review Date: To be reviewed at least annually or upon significant change. Please note reviews are not recorded in version control table but in the document review file.				
Responsible Manager: David Smith				
This document is controlled. If you would like to suggest amendments to this document, please contact the document author. If printed this document is uncontrolled. For the latest copy please see the document owner.				
This document is public.				