Security Policy

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

- Develop, implement, and review policies and processes for physical and information security.
- 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 assets, information and information systems against theft, abuse and other forms of harm and loss.
- Provide a safe and secure environment for client's assets 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 can continue their services even if an incident occurred.
- Work with employees to maintain the responsibility for, ownership of, and knowledge of physical and information security such that the risk of security incidents is reduced.
- Communicate all policies, procedures and working instructions to Customers, Employees, and all other interested parties.
- Continually improve both physical and information security systems to protect against any potential breaches.

The directors and all employees of S2S are committed to an effective Security Management System in accordance with its strategic business objectives, to protect physical assets and digital information, its infrastructure, and personnel from unauthorized access, damage, theft, or any other potential threats.

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

Physical and information security will be ensured by this policy, management systems and a set of working instructions. To secure operations at S2S's premises, even after a serious incident, S2S shall ensure the availability of business 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 employees or contract restrictions and cancellations for suppliers and third parties.

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

S2S will conduct regular audits to ensure compliance with this policy.

S2S will update this physical security policy to adapt to changing threats and technologies.

Rachel Hall
Operations Director

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
1.3	17/11/20	David Smith	Live	Review, copied to uSecure for internal S2S staff
1.4	04/04/2024	Keeley Lambert	Live	Rebranding & Merge InfoSec and Physical Policy together
Approved Date: 04/04/2024				
Approved By: Rachel Hall				
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: Keeley Lambert				
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.				