S2S ELECTRONICS LTD

Security Policy

ISO 27001:2015 5.2

S2S is committed to safeguard 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**
- **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.

SECURITY STRATEGY

S2S's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks though 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, defense against malicious activities, system and information access controls, physical security, staff vetting, incident management and reporting.

SECURITY OBJECTIVES

S2S have different security objectives at different levels of the business these are shown

High Level security objectives

To work with internal and external interested parties to ensure the assets within S2S, both S2S and customer owned remain secure at all times.

Medium level security objectives

To assess the risks that apply to S2S and put controls in place that minimise the risks to an acceptable level. These objectives will change depending on the risk assessments at the time. The current objectives are listed on the S2S noticeboard.

A. Dukinfield
Managing Director