Information Security Policy Statement

This policy has been approved by Sustainable Tech 4 Good Group Limited (ST4G) & Veritas Digital Services Limited (VDS), and any amendments require approval by Sue Gowling. The policy provides the information required to enable you to ensure your area of business complies with the Policy. Support and guidance is offered by managers, which includes training, policies and guidance. Information Security is not a new requirement, and to a large extent this policy formalises and regulates existing good practice. This policy provides a framework for the management of information security throughout ST4G/VDS.

It applies to all those with access to ST4G/VDS information systems, including staff, visitors and contractors, any system attached to ST4G/VDS computer or telephone networks and any systems supplied to ST4G/VDS. Also, all information (data) processed by ST4G/VDS pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form, any communications sent to or from ST4G/VDS and any information (data) held on systems external to ST4G's network. In addition, all external parties that provide services to or for ST4G/VDS, in respect of information processing facilities and business activities, and principle information assets including the physical locations from which ST4G/VDS operates.

Top Management at ST4G/VDS recognise the important role information security plays in data protection and privacy. The potential loss or unauthorised disclosure of information has the potential to damage ST4G/VDS' reputation and cause financial loss. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard copy form.

In order to meet these aims, we are committed to security controls that conform to best practice. We carry out information security risk assessment at regular intervals. Awareness and education is provided via training. We keep up to date and circulate any new and relevant legal and regulatory information. Any breaches of information are recorded and reported to the relevant people and authorities. This policy and other supporting policies shall be communicated as necessary throughout ST4G/VDS to meet its objectives and requirements.

Sue Gowling has ultimate responsibility for information security within ST4G/VDS. Managers are responsible for information security in their own business areas, and each employee has a duty to protect information in the same way. Information will be restricted to contracted third party suppliers and other external parties to the minimal required to complete their function.

Relevant legislation in connection with this policy includes, but is not limited to The EU General Data Protection Regulation (2016), The Computer Misuse Act (1990), The Data Protection Act (1998), The Regulation of Investigatory Powers Act (2000), The Telecommunications (Lawful Business Practice) (Inception of Communications) Regulations (2000), and the Freedom of Information Act (2000)

Approved By: Sue Gowling - Founder

Date: 29th November 2019

Reviewed: 27th January 2026