INFORMATION SECURITY POLICY

TRAC International Ltd and Subsidiary Companies (TRAC) provides first class products and services worldwide. In order to carry out our business(es), we recognise the importance of our duty to protect the security of company information and assets. We take this duty seriously and are committed to taking all reasonable measures to ensure the appropriate technical and organisational measures are in place to prevent:

- Unauthorised or unlawful processing of company information and systems.
- Accidental loss or destruction of company information and systems.

In particular, TRAC shall ensure:

- Senior management commitment for the provision of adequate resources to ensure security of the system.
- A competent IT Department and external provider(s) responsible for the security of the system on behalf of the Group at the direction of Senior Management.
- Robust security controls are in place such as firewalls, password protection, assigned access and encryption-based software; and that these controls are kept current.
- That measures are in place to verify that implemented security controls are providing the intended level of security.
- The provision of adequate disaster recovery processes and contingency measures to reduce interruption to TRAC activities; including the testing of such systems (e.g. emergency scenarios, data recovery and penetration testing).
- Authorisation of software and relevant level of access required for individuals to carry out their duties.
- That all sensitive information is clearly identified, accessed, stored and processed securely in line with company confidentiality agreements and privacy notices.
- That any information links with third parties are fully authorised and risk assessed prior to implementation.
- Training to ensure that all staff are aware of their responsibilities in relation to confidentiality, information stored on removable media and remote access to TRAC's systems as is appropriate to an individual's role.
- Efficient change management processes; including the necessary steps to be taken when a person is no longer employed by TRAC to ensure access to systems, software and social media accounts is revoked where relevant.
- Appropriate measures are in place to prevent and detect any unauthorised removal of information, systems and software.

Appropriate risk analysis is undertaken by top management to identify company assets and the level of protection and associated testing that is needed. Top management shall review at least annually TRAC's information security environment and any additional measures that are needed to ensure this policy. Appropriate action shall be taken to remedy any vulnerabilities identified as part of management review/risk analysis.

All employees of TRAC shall ensure that company activities are carried out in a professional manner and will hold all company and customer information in strictest confidence. The violation of any aspect of this policy may result in disciplinary action, up to, and including termination of employment, in accordance with our disciplinary and grievance processes. This policy should be read in conjunction with TRAC's Privacy/Fair Processing Notice (TRACPN 01) and Internet and Social Media Policy (TRAC POL C09).

Implementation of this policy is the responsibility of the relevant company Managing Director, who is ultimately responsible for all Company operations.

INFORMATION SECURITY POLICY

For and on behalf of TRAC International and subsidiary companies:

Managing Director	K. Stephen	**Signature**
Date	28th January 2021