Information Security Policy Statement

The objective of information security is to ensure business continuity by preventing loss of information. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversations or over the telephone. The protection of information from unauthorised disclosure or intelligible interruption is imperative, as is safeguarding the accuracy and completeness of information by protecting against unauthorised access.

The purpose of the policy is to protect the Company's information assets from all threats, whether internal or external, deliberate or accidental, and to ensure that information and vital services are available to users when they need them. It is the policy of the Company to use all reasonably practicable measures to ensure that:

- Information will be protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory and legislative requirements will be met.
- Business Continuity plans will be produced, maintained and tested.
- Requirements for availability of information and information systems will be met.

We have systems in place to follow the three fundamental principles of information security - confidentiality, integrity and availability. We ensure that information and information systems are protected from unauthorised use, access, modification and removal, whether this is held on our computer systems and server, or in confidential locked file cabinets in our Head Office. This includes but is not limited to:

- Authorised access only with security systems in place at Head Office including fob system/entry codes/restricted areas.
- High level company server areas for confidential data - restricted access to authorised personnel only.
- Robust cyber security measures in place for our network, server and computer systems, ensuring only authorised personnel have access to information.
- Accreditation with Cyber Essentials Scheme.
- Documentation destruction and disposal carried out by certified confidential shredding contractor.

This statement should be read in conjunction with QS 15 Internet Security Procedure and all managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff. It is the responsibility of each employee to do everything reasonable within their power to ensure that this policy is carried into effect. Controls are already in place which include the requirements of legislation such as the Companies Act, Data Protection Act and General Data Protection Regulations (GDPR).

Information Security Training:

- 100% of Office and Operations Staff who deal with Personal Data and protection of data in any form undergo full training courses on GDPR.
- 100% of all employees have been trained through induction/briefing/toolbox talk on Information Security and GDPR policy and procedure, to a level appropriate to their role.
- Information is sent out by email to all employees detailing any changes to Data Protection Laws, along with our Privacy Statement, Policy, Procedure and Data Processing Information.

Breaches of Internet Security:

Any breach of information security, actual or suspected, should be reported to, and investigated by, the Head of Digital & Technology, who will report to the appropriate Senior Leadership personnel.

The CEO shall review this policy annually or following significant changes.

Brusk Korkmaz
Chief Executive Officer
Hercules Site Services PLC

Approved on: 01/01/2022