INFORMATION SECURITY MANAGEMENT POLICY

The purpose of the policy is to protect our business information assets from all threats, whether internal or external, deliberate, or accidental. The objective of information security is to ensure business continuity by preventing breaches of security and to continually improve our information security system.

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
- Company requirements for availability of information and information systems will be met

This statement supports the company's procedures and processes relating to…………

- the use of the internet & email
- the use of computer systems
- Data Protection – UK-GDPR
- hard copies of information

Information is a valuable company asset which can be collected, processed, store and transmitted. It can exist in many forms e.g. printed or written on paper, as an electronic record, as a photograph, film, video or spoken. Information can come from a range of resources e.g. information system infrastructure, proprietary knowledge, end users of systems, databases, technical and production skills, filing cabinets, documents, and records.

All managers are directly responsible for implementing this policy within their 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 information security policy is carried into effect.

Breaches of information security, actual or suspected, should be reported to, and investigated by the Information Security Management System Manager.

Information management security system objectives are reviewed at the annual management review meetings or when significant changes take place to ensure the system meets the requirements of stake holders BS EN ISO/IEC 27001 (latest edition) and any statutory, regulatory or compliance obligations.

Changes to this policy in response to changing demand, both operational and legislative, will be available on the company website. This policy will be communicated to all employees and organisations working on our behalf and displayed at our offices and on our intranet and is available to defined interested parties.

This Policy is authorised for issue by:

Andy Vincent
IT & Digital Director
31/03/2023