Security Policy

Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax or email, and stored on various types of media.

We have implemented an Information Security Management System to ensure business continuity and to prevent security incidents. The purpose of the management system is to protect the company's information assets from all identified threats, whether internal or external, deliberate, or accidental.

It is our policy, approved by the Directors, to ensure that:

- Information will be protected against unauthorised access.
- Confidentiality of information will be assured.
- Regulatory and legislative requirements together with any contractual security obligations will be met.
- Integrity of information will be maintained.
- Business requirements for the availability of information systems will be met.
- The criteria against which risks to information security are evaluated are included in the information Security Risk Assessment
- Information Security training will be provided.
- All breaches of Information Security, actual or suspected, will be reported, investigated and the appropriate corrective action taken.
- Procedures and instructions will be produced to support the objectives of this policy.
- It is the responsibility of each employee to adhere to the Information Security Policy.
- Objectives and targets will be set and monitored to achieve continual improvement in information security management systems.
- All Managers are directly responsible for implementing this policy within their business areas and for adherence by their staff.

Chris Knowles
Managing Director