

The purpose of this policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental.

The policy covers Physical Security of premises and encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written on paper, stored on any device or media capable of data storage or spoken in conversation or over the telephone. 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 adhere to the policy at all times. Disciplinary procedures may be initiated in those instances where employees fail to abide by this security policy.

Our statement of general policy is:

- To identify and evaluate risks to the information assets of the company
- To protect information against unauthorised access and malicious damage
- To assure confidentiality of information
- To maintain integrity of information
- To meet regulatory, legislative, business and contractual security obligations
- To produce, maintain and test business continuity plans
- To provide staff with sufficient information security training
- To facilitate continual improvement in information security
- To communicate this policy to people working under the control of the company
- To provide a framework for the setting and monitoring of objectives and targets
- To review and revise this policy as necessary at regular intervals

All breaches of information security, actual or suspected, are reported immediately and investigated.

Signed



Oliver J Briggins
Managing Director

Approved:
27th September 2021

Review date
27th September 2023