Information Security Policy

The Company will seek to ensure that the confidentiality, integrity and availability of its information is maintained by implementing best practice to minimise risk.

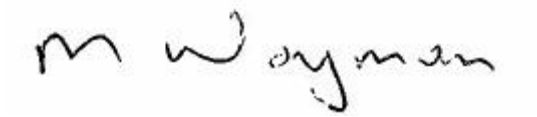
This Policy has been developed to protect all systems within the Company to an adequate level from events which may jeopardise Company activity. These events will include accidents as well as behaviour deliberately designed to cause difficulties.
The objective of Information Security is to ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.
The purpose of security in this information system, computer installation or network is to preserve an appropriate level of the following:-

Confidentiality **-** the prevention of the unauthorised disclosure of information
Integrity **-** the prevention of the unauthorised amendment or deletion of information
Availability **-** the prevention of the unauthorised withholding of information or resources

The level of security required in this particular system depends upon the risks associated with the system, the data held on the system and the working environment of the system.
This policy applies to all information held in both manual and electronic form.
The purpose of the Policy is to protect the Company's information assets from all threats, whether internal or external, deliberate or accidental; it is also a method of promoting continual improvement in all areas of Information Security and this is evaluated for effectiveness by the company management team.

The Company Directors has approved the Information Security Policy and has delegated responsibility for its upkeep and co-ordination to the Managing Director. It is the policy of the Company to ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Information Security Training will be provided
- All breaches of Information Security, actual or suspected, will be reported and investigated
- Standards will be produced to support the policy. These include virus controls and passwords
- Business requirements for the availability of information and information systems will be met
- The Managing Director has direct responsibility for maintaining the policy and providing advice, and guidance on its implementation
- 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 Information Security Policy
  ISMS Objectives are identified, set and reviewed at least annually.



M Wayman
Executive Director
February 2020