Cyber security policy

OBJECTIVE

The purpose and objective of this Information Security Policy is to protect the company's information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

POLICY

- The [Chief Executive Officer] or [Managing Director] has approved the Information Security Policy.
- It is the Policy of the [company] to ensure that:

  a. Information will be protected from a loss of: confidentiality (note 2), integrity (note 3) and availability (note 4).

  b. Regulatory and legislative requirements will be met (note 5).

  c. Business continuity plans will be produced, maintained and tested (note 6).

  d. Information security training will be available to all staff.

  e. All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.

- Guidance and procedures will be produced to support this policy. These may/will include risk assessment, information classification, data protection, credit card handling (PCI), incident handling, information backup, system access, third party services (supplier due diligence), malware controls, mobile device security & remote working, passwords and encryption.
- The role and responsibility of the designated Information Security Manager (note 7) is to manage information security and to provide advice and guidance on implementation of the Information Security Policy.
- The designated owner of the Information Security Policy [name] has direct responsibility for maintaining and reviewing the Information Security Policy.
- All managers are directly responsible for implementing the Information Security Policy within their business areas.
- It is the responsibility of each employee to adhere to the Information Security Policy.

NOTES

1. Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.
2. Confidentiality: ensuring that information is accessible only to authorised individuals.
3. Integrity: safeguarding the accuracy and completeness of information and processing methods.
4. Availability: ensuring that authorised users have access to relevant information when required.
5. This includes the requirements of legislation such as the Companies Act, the Data Protection Act, the Computer Misuse Act and the Copyright, Design and Patents Act.
6. This will ensure that information and vital services are available to users whenever they need them.
7. Depending on the size and nature of the business this may be a part or full-time role for the nominated person.