Information Security Management Policy

- The policy's goal is to protect the organisation's informational assets against all internal, external, deliberate or accidental threats.
- Management have approved the information security policy & shall strive to continually improve the ISMS.
- The Information security policy and associated objectives ensures that:
    - Information will be protected against **unauthorised access;**
    - **Confidentiality** of information will be assured;
    - **Integrity** of information will be maintained;
    - **Availability** of information for business processes will be maintained;
    - **Legislative and regulatory** requirements will be met;
    - **Business continuity plans** will be developed, maintained and tested;
    - **Information security training** will be available for all employees;
    - **All actual or suspected information security breaches** will be reported to the Chief Information Officer and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords, continuity plans and effective risk management.
- Business requirements for availability of information systems will be met.
- The Senior Management Team are responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with contractual security obligations is mandatory.
- Compliance with the Information Security Policy is mandatory.

Approved by: CEO **Date:22/01/19**
Document Ref: P-IS-001

<u>This policy shall be reviewed annually as a minimum and available to external parties upon request.</u>