OP.2 Information Security Management System Policy

Intent: The objective of the ISMS policy is to mitigate the likelihood and mitigate the risk of security incidents and reducing their potential impact.

ISO 27001 Ref: Clause 5.2

POLICY

- The policy's goal is to protect the organisation's informational assets against all internal, external, deliberate or accidental threats whilst satisfying all applicable requirements related to information security.
- The Managing Director has approved the information security policy.
- 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 Information Security Manager and will be thoroughly investigated.
- Procedures exist to support the policy, examples include but are not limited to; virus control measures, passwords, continuity plans and effective risk management.
- Business requirements for availability of information systems will be met.
- The Managing Director is responsible for maintaining the policy and providing support and advice during its implementation. There will be an annual management review to verify conformity and discuss system issues.
- The Managing Director is directly responsible for implementing the policy and ensuring staff compliance in the respective departments.
- Compliance with contractual security obligations.
- Compliance with the Information Security Policy is mandatory.
- There shall be commitment to continually improve the Information Security Management System