For sample purposes only

XYZ'S ISMS POLICY

OBJECTIVE

XYZ's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. XYZ shall ensure that all information that are disbursed or produced by XYZ have absolute integrity. XYZ shall guarantee that all relevant information are managed and stored with appropriate confidentiality procedures.

POLICY

- The purpose of the Policy is to protect the organization's information assets[1] from all threats, whether internal or external, deliberate or accidental.
- The Managing Director has approved the Information Security Policy.
- It is the Policy of the organization to ensure that:
    - Information should be made available with minimal disruption to staff and the public as required by the business process[2];
    - The integrity of this information will be maintained[3];
    - Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured[4];
    - Regulatory and legislative requirements will be met[5];
    - A Business Continuity Management Framework shall be made available and Business Continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. Business continuity plans should be maintained and tested[6];
    - Information security education, awareness and training will be made available to staff[7];
    - All breaches of information security, actual or suspected, will be reported to, and investigated by the relevant authorities not limited to System Administration and Incident Response[8];
    - Appropriate access control will be maintained and information is protected against unauthorized access.

- Policies, Procedures and Guidelines not limited to Information Security will be made available in both hardcopy and online format through an intranet system to support the ISMS Policy.

- Internal Audit Unit has direct responsibility for maintaining the ISMS Policy and involved with writing and/or managing the development of relevant policies, procedures and guidelines not limited to information security.

- All managers are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.

- It is the responsibility of each member of staff to adhere to the ISMS Policy.

- Information security is managed through XYZ's Risk Management framework.

    - The availability of information and information systems will be met as required by the core and supporting business operations.

---

[1] Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the telephone.

[2] This will ensure that information and vital services are available to users when and where they need them.

[3] Safeguarding the accuracy and completeness of information by protecting against unauthorized modification.

[4] The protection of valuable or sensitive information from unauthorized disclosure or unavoidable interruptions.

[5] This will ensure that the organization remains compliant to relevant business, national and international laws and it include meeting the requirements stated in legislations such as the Malaysian Copyright Act 1987, Companies Act and the Data Protection Act.

[6] Business Continuity Management should be implemented effectively to ensure continuity of business operations in the event of a crisis or disaster.

[7] Ensure that relevant and effective trainings are provided to staffs.

[8] Ensure that the staff understand their roles and responsibilities in handling incidents and have a comprehensive and well-tested incident response plan ready.

The policy will be reviewed by XYZ's ISMS Forum after a one-year duration for update.