LABUAN FINANCIAL SERVICES AUTHORITY'S
INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

BACKGROUND

Information Security Management System (ISMS) is based on the standard IS0 / IEC 27001: 2013 Information Technology – Security Techniques – Information Security Management System. Labuan FSA is committed in ensuring that all aspects of information security are complied with the standards and provide guarantee to all stakeholders that relevant information is protected and safe from damage, loss or misuse.

OBJECTIVE

The overall objective of an information security program is to protect the company's registration: COR@L information and system in Labuan FSA that support the operations and assets of the organisation in ensuring that Registrar of Companies' (ROC) core operations to operate with minimal disruptions and the following three (3) main security objectives can be realized for their information:

- **Confidentiality**

  Protecting information from unauthorised access and disclosure.

- **Integrity**

  Assuring the reliability and accuracy of information and IT resources by guarding against unauthorised information modification or destruction.

- **Availability**

  Defending information systems and resources to ensure timely and reliable access and use of information.

In this regard, Labuan FSA shall ensure that all ROC's information that are disbursed or produced by LFSA have absolute integrity. LFSA shall guarantee that all the relevant information is managed and stored with appropriate confidentiality procedures.

LABUAN FINANCIAL SERVICES AUTHORITY'S

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) POLICY

PURPOSE

The purpose of the Policy is to protect the organisation's information assets[1] from all threats, whether internal or external, deliberate, or accidental.

The Management Committee (MC) has approved the Information Security Policy.

The Information Technology Communication Unit has the responsibility in ensuring the policy is implemented and adhered to.

POLICY

The ISMS Policy is a document which acts as the fundamental principle of the information security management in Labuan FSA in ensuring the following to be adhered to:

- **Confidentiality**
  - ➢ Confidentiality of information not limited to research, third parties, personal and electronic communications data will be assured[2];
  - ➢ All Head of Units (HOUs) 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.

- **Integrity**
  - ➢ The integrity of this information will be maintained[3];
  - ➢ Appropriate access control will be maintained and information is protected against unauthorised access.
  - ➢ Information security education, awareness and training will be made available to staff;
    - ➢ 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[4];

---

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

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

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

- **Availability**
  - ➢ Information security is assessed through Labuan FSA's Enterprise Risk Management framework.
  - ➢ The availability of information and information systems will be met as required by the core and supporting business operations.
  - ➢ Information should be made available with minimal disruption to staff and the public as required by the business process[5];
  - ➢ Regulatory and legislative requirements will be met[6];
  - ➢ 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.

---

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

[6] This will ensure that the organisation 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 2016 and the Personal Data Protection Act 2010.