LABUAN FINANCIAL SERVICES AUTHORITY
(LEMBAGA PERKHIDMATAN KEWANGAN LABUAN)

Reference No. : 341/2026/ALL
Date : 11 November 2026

Association of Labuan Banks (ALB)
Labuan Investment Banks Association (LIBA)
Labuan International Insurance Association (LIIA)
Association of Labuan Trust Companies (ALTC)
Labuan Money Brokers
Labuan Fund Managers
Labuan Securities Licensees
Labuan Credit Token Business
Labuan Exchanges
Labuan Payment System

Dear Sir/Madam,

Reminder on Cybersecurity Vigilance and Risk Management

Recent cyber incidents across Asia, including those affecting financial institutions and third-party service providers, highlight the growing frequency and sophistication of cyber threats. Attacks involving phishing, ransomware, malware and social engineering continue to pose risks of data breaches, financial losses and operational disruptions.

2. In this regard, Labuan FSA reminds all Labuan financial institutions (LFIs) to remain vigilant and strengthen their cybersecurity safeguards and operational resilience. LFIs are expected to manage cybersecurity risks as part of their overall risk management, with controls proportionate to the nature and scale of their operations. LFIs must regularly review the effectiveness of their cybersecurity measures, including but not limited to the following areas:

(i) Data protection and access controls – Restrict access to authorised personnel through strong authentication and appropriate access privileges. Ensure sensitive data is adequately protected during storage, transmission and disposal;

(ii) System security – Apply security updates and address identified vulnerabilities promptly. Maintain secure backups of critical data and regularly test their integrity and recoverability;

(iii) Threat detection – Establish effective monitoring mechanisms to detect, investigate and escalate suspicious activities promptly. Pay particular attention to unusual system access, unauthorised transactions and potential indicators of cyber intrusions to enable timely intervention;

(iv) Employee awareness – Conduct regular cybersecurity awareness training to equip staff in recognising phishing attempts, social engineering tactics and other emerging cyber threats. Reinforce safe practices in handling suspicious emails, links, attachments and requests for sensitive information, including appropriate verification and reporting procedures;

(v) Third-party security – Ensure appropriate cybersecurity safeguards and ongoing monitoring of service providers with access to critical systems or sensitive information. Assess potential risks arising from third-party dependencies and security weaknesses; and

(vi) Incident response and recovery – Maintain and regularly test incident response and business continuity plans, including clear escalation, communication and recovery procedures to minimise operational disruptions.

3. In the event of a cyber incident, LFIs must act promptly to contain the impact, activate their response and continuity plans, and notify Labuan FSA through expeditious means (e.g. email, phone call, etc.) in line with its applicable requirements, using the following contact details:

Supervision Department
Labuan Financial Services Authority
Level 17, Main Office Tower
Financial Park Complex
Jalan Merdeka
87000 Federal Territory of Labuan, Malaysia

Telephone no: 03 8873 2000
Facsimile no: 03 8873 2209
Email: sed@labuanfsa.gov.my

Yours sincerely,



Syahrul Imran Mahadzir
Deputy Director General
Regulatory Oversight & Technology
Labuan Financial Services Authority