1. Labuan FSA is introducing the Guidelines on Payment System Operator to establish a clear and structured regulatory framework for entities undertaking payment system and to provide clarity on the provision of the safekeeping and administration of digital assets in Labuan IBFC.

2. This exposure draft sets out Labuan FSA's regulatory requirements for the application, operational and other requirements in Labuan IBFC, aims to provide clarification and ensure that payment system operations in Labuan IBFC remain safe, efficient, transparent, and aligned with international best practices while supporting innovation in digital financial services.

3. In this regard, Labuan FSA welcomes and values feedback on the requirements of the exposure draft. The comments or inputs may encompass suggestions, recommendations and alternatives, which should be supported with clear rationale, practicality and relevance for Labuan FSA's consideration. Feedback shall be submitted electronically to Labuan FSA using the response template by **6 March 2026** to bpu@labuanfsa.gov.my.

4. Should you require any clarification on the exposure draft, please contact the following officers:
   (i) Mr. Razeen Dzarif Al-Hasyeer
   (razeen@labuanfsa.gov.my) (03-8873 2135)
   (ii) Ms. Khairunnisa Abdul Karim
   (khairunnisa@labuanfsa.gov.my) (03-8873 2016)
   (iii) Ms. Doreen Fadli
   (doreen@labuanfsa.gov.my) (03-8873 2015)

GUIDELINES ON PAYMENT SYSTEM OPERATOR

1.0 Introduction

1.1 As the digital finance landscape continues to evolve, payment services increasingly rely on technology-driven platforms that facilitate the initiation of transferring, clearing and settlement of funds and digital assets. A well-functioning Payment System Operator (PSO) is crucial for the efficient operation of the financial system as well as to support the needs of the economy as any disruptions may have broader system-wide implications.

1.2 Over the past decade, payment system has evolved and expanded significantly particularly through the growth of electronic money, driven by the proliferation of mobile technologies such as mobile applications, the digitalisation of financial services, and shifts in consumer behaviour. The form of electronic money has progressed from traditional stored value cards to network-based solutions such as online accounts or e-wallets.

1.3 Within this evolving landscape, the safekeeping and administration of digital assets also play a crucial role in completing the digital asset ecosystem. This function is essential to ensure that digital assets are properly held, managed, and safeguarded, thereby providing the foundation for trust, transparency, and investor confidence in digital markets.

1.4 The Guidelines aims to provide clarity on the scope of business, application and operational requirements for entities undertaking the payment system in the Labuan International Business and Financial Centre (Labuan IBFC).

2.0 Applicability

2.1 The Guidelines is applicable to any person[1] approved by Labuan Financial Services Authority (Labuan FSA), including new applicants, to carry on payment system operator business pursuant to Section 171 of *Labuan Financial Services and Securities Act 2010 (LFSSA)* or Sections 136 of *Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA).*

3.0 Legal Provision

3.1 The Guidelines is issued pursuant to Section 4A of the *Labuan Financial Services Authority Act 1996 (LFSAA)* to clarify the provisions of Part V of LFSSA.

3.2 Any person who fails to comply with the Guidelines may be imposed with an administrative penalty under Section 36G of the LFSAA and/or other enforcement actions provided under the LFSAA.

3.3 The Guidelines should be read together with the requirements of the relevant Guidelines and Circulars including those listed under **Appendix I**.

4.0 Effective Date

4.1 The Guidelines shall come into effect immediately and will remain effective and applicable unless amended or revoked.

4.2 All approvals granted by Labuan FSA relating to Labuan payment system operator business before the effective date of this Guidelines remain valid unless revoked and are subjected to the new requirements of this Guidelines upon its effective date.

5.0 Interpretation

5.1 For the purpose of the Guidelines:

(a) **Digital assets** refer to a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes;

(b) **Electronic money or "e-money"** refers to any payment instrument, whether tangible or intangible, that:

[1] As defined in Section 2 of LFSSA which includes a corporation, partnership, a body of persons, corporate or unincorporated and a corporation sole.

(i) stores funds electronically in exchange for funds paid to the issuer[2]; and

(ii) is able to be used as a means of making payment to any person other than the issuer;

(c) **Instrument** refers to any password, code, cipher, cryptogram, private cryptographic key or other instrument that enables a person:

(i) to control access to one or more digital assets; or

(ii) to execute a transaction involving one or more digital assets;

(d) **Payment instrument** refers to any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to make any payment;

(e) **Safekeeping and administration of digital assets** refers to providing services of storing, holding, controlling and/or maintaining digital assets or instruments enabling transfer of digital assets, on behalf of a customer including any other services as approved by Labuan FSA.

Question 1
Do you have any comments on the above definitions whether they are sufficiently clear, appropriate, and consistent with existing regulatory and market practices. If yes, please provide your recommendation and justification.

6.0 Eligibility

6.1 The applicant for an approval to carry on payment system in Labuan IBFC shall have the following:

(a) the applicant, its directors, person in control and senior management are fit and proper which include having a sufficient number of experiences[3], relevant qualifications or expertise in financial technology, risk management and compliance, and demonstrate the capacity to oversee operations involving emerging payment technologies, as well as good financial standing;

[2] "Issuer" means any person, acting alone or under an arrangement with another person, who undertakes to be responsible for the payment obligation in respect of a payment instrument resulting from a user being issued with or using the payment instrument

[3] Typically, Labuan FSA would expect the applicant to have at least three years of experience in payment system or its related activities. Notwithstanding this, all applicants would be assessed holistically based on their own merits of the application.

(b) adequate financial, human and other[4] resources for its operation and commensurate with the nature, scale, complexity and diversity of the business;

(c) a credible and viable business plan that sets out the approach to implement the proposed business objectives or operations. Its management and operational structure should be adequate for the intended business plan. Where the applicant is part of a group, Labuan FSA may assess the management and operational structure of the group, or related corporation, to ensure that Labuan FSA can effectively oversee the applicant if approval is granted; and

(d) the ability to carry out its obligations as set out in the Guidelines and to manage risks associated with its business and operations, including demonstrating the processes and contingency arrangements in the event it is unable to continue its operations.

Question 2
Do you have any comments on the eligibility criteria under this section? If yes, please provide your recommendation and justification.

7.0 Permissible Activities

7.1 Pursuant to Section 86 of LFSSA and Section 2 of LIFSSA, payment system means any system or arrangement for the transfer, clearing or settlement of funds or securities but excludes those who are:

(a) a payment system established or operated by the Central Bank or operated on behalf of the Central Bank, under the Central Bank of Malaysia Act 2009;

(b) a clearing house defined under the Capital Markets and Services Act 2007;

(c) an in-house payment system operated by a person solely for his own administrative purposes that does not transfer, clear or settle of funds or securities for third parties; and

(d) a system that solely facilitates the initiation payment instructions.

[4] For example, technological and infrastructure resources.

7.2 For the avoidance of doubt, the Guidelines clarifies that the payment system under paragraph 7.1 may include the following:

(a) The transfer, clearing or settlement of digital assets, including the safekeeping and administration of digital assets; and

(b) Provision of e-money services.

Question 3

(i) This Guidelines clarifies the definition of payment system under LFSSA and LIFSSA includes the provision of digital assets services including the safekeeping and administration of digital assets as well as e-money services. Do you have any comments on the scope of permissible activities, whether it is in line with the current market practices and legal standpoint?

(ii) Any other services under the safekeeping and administration of digital assets may include ancillary or incidental services, such as the acceptance and withdrawal of a customer's digital assets. The acceptance of customer's digital assets refers to digital assets received under a contract for the provision of a service and does not tantamount to bank deposits. Do you have any comments on this and should there be any other examples of ancillary or incidental services that are relevant to this business activity? If yes, please provide your recommendation and justification.

8.0 Responsibilities of the Board and Senior Management

8.1 Board of Directors

The board of directors shall:

(a) Have a board charter that sets out the mandate, responsibilities and operating procedures, including the matters reserved for the board's decision and its committees, if applicable.

(b) Establish a board committee, where relevant, to support the board in carrying out its duties and responsibilities.

(c) Have overall responsibility for safeguarding the safety, efficiency, and reliability of the payment system, including:

(i) approve the strategic objectives, business plans and key policies, including their associated risk appetite;

(ii) approve and oversee all key policies including those relating to

risk management, internal controls and compliance with the with applicable laws and regulatory requirements as well as industry best practices;

(iii) oversee the appointment, performance, remuneration, and succession planning of senior management to ensure that the board is satisfied with the collective competence of senior management in effectively managing the operations of the PSO;

(iv) ensure that clear roles, responsibility and accountability are established and effectively communicated throughout the organisation;

(v) establish and provide oversight of the risk management function and material risk decisions, including ensuring that appropriate risk management policies, processes and infrastructure are in place and effectively implemented to manage various risk profiles;

(vi) ensure that internal control functions operate independently and effectively;

(vii) approve and oversee Business Continuity Management (BCM) and ensure that it is reviewed and updated, particularly when there are material changes to the size, nature and complexity of the payment system's operations that may significantly affect those plans;

(viii) promote timely and effective communication between the PSO and Labuan FSA on matters that affect, or potentially impacting the safety, efficiency and reliability of the PSO; and

(ix) ensure compliance with legal and regulatory obligations.

(d) Able to devote sufficient time to their roles and maintain a sound understanding of the PSO's business as well as relevant market and regulatory developments.

8.2 Senior Management

The senior management shall:

(a) Comprise individuals with the requisite skills, competencies and experience to effectively support the operation and risk management of the PSO, including individuals with appropriate technological expertise to

provide guidance on the PSO's technology plans and operations.

(b) Implement business and risk strategies and other strategic plans, including technology plans and the related technology policies and procedures, in accordance with the directions set by the Board.

(c) Establish and maintain policies and procedures including those relating to risk management, internal controls and compliance with the applicable laws and regulatory requirements as well as industry best practices to:

(i) effectively and efficiently manage actual and potential conflicts of interest;

(ii) monitor the transfer of digital assets or instruments to detect non-compliance with applicable laws and regulatory requirements;

(iii) address and resolve complaints relating to the services provided;

(iv) ensure compliance with all applicable laws and regulatory requirements;

(v) define and oversee the PSO's business plan and strategy in a manner that is appropriate to its objective, size, structure and risk profile;

(vi) ensure that the PSO possesses the necessary capabilities including technological capabilities and support, secure infrastructure, and adequate resources to carry out its business; and

(vii) ensure that robust assessments are conducted on any deviations from legal and regulatory requirements as well as internal policies and procedures. including addressing any supervisory concerns and monitoring the progress of remedial actions taken to resolve them, with material information to be reported to the Board in a timely manner.

(d) Ensure that designated staff who are independent of day-to-day technology operations shall be responsible for the identification, assessment and mitigation of technology risks.

(e) Manage risks associated with the business of a PSO including conducting periodic evaluation of its risk management process.

(f) Provide timely, accurate and sufficient information to the Board on the PSO's operations.

(g) Ensure all records of customer transactions and all records that adequately explain the financial position and the business are accurate, properly secured and retained in accordance with the specified timeline.

Question 4
Do you have any comments on the responsibilities of the board and senior management including any requirements that need to be included or clarified? If yes, please provide your recommendation and justification.

9.0 Risk Management Framework

9.1 The PSO shall establish a risk management framework to identify, assess, monitor, control and report all material risks to which it may be exposed including the policies, procedures and systems that enable the identification, measurement, control and ongoing monitoring of all relevant and material risks that a PSO bears from and poses to, its participants and other relevant parties.

9.2 The risk management framework shall include at least the following:

(a) strategies developed to identify, assess, monitor and mitigate all material risks;

(b) policies and protocols relating to management and controls of all material risks;

(c) methodologies for assessing all material risks; and

(d) a reporting system for all material risks to senior management and Board.

9.3 In addition, in lights of the evolving cyber threat landscape, the PSO shall develop a Cyber Risk Management Framework (CRMF) that sets out the PSO's governance arrangements for managing cyber risks, its cyber resilience objectives and risk tolerance.

9.4 The CRMF shall include at least the following:

(a) actively manage software and hardware inventories and ensure up-to-date records are properly maintained;

(b) ensure that critical systems, applications and data are backed up and protected against deliberate erasure or encryption;

(c) perform continuous and integrated security monitoring of the IT infrastructure (network, systems and endpoints) with effective collection, analysis and retention of audit logs;

(d) adopt multi-factor authentication for all access;

(e) establish and periodically test incident response programs to prepare for, detect and respond promptly to cyber-attacks; and

(f) provide adequate and regular technology and cybersecurity awareness training programmes for all staff, including the board, that reflect current cyber threats.

Question 5
Do you have any comments on risk management and the CRMF? If yes, please provide your recommendation and justification.

10.0 Digital Assets Wallet Management

10.1 Digital asset storage

(a) Establish and maintain a sufficient and verifiably secure medium of storage for the safekeeping of customers' digital assets.

(b) Conduct a risk-based analysis to determine appropriate storage methods for digital assets, including the use of different types of digital assets wallets[5].

(c) Have in place effective security mechanisms for digital assets, including adopting measures such as multi-factor authentication requirements.

(d) Provide detailed information on the methodologies governing the transfer of digital assets between different types of digital assets wallets. The transfer mechanisms shall be properly documented and audited.

(e) Have and maintain appropriate certifications, where applicable, as required under industry, best practices applicable to the safekeeping of digital assets, at all times.

[5] Such as hot, cold or warm wallets

(f) Ensure that all customers' digital assets are properly segregated from the PSO's own assets and safeguarded against conversion or inappropriate use by any person.

(g) Establish systems and controls to maintain accurate and up-to-date records of customers' digital assets held and transacted including the following:

(i) transaction timestamp;

(ii) details of any transaction including the purpose of the transfer, the amount involved and particulars of the counterparty;

(iii) relevant signatories and transaction approval/rejection evidence;

(iv) account balances;

(v) transaction value; and

(vi) any other information as may be specified by the Labuan FSA.

10.2 Seed or key generation, storage, and use

(a) Have in place effective policies and procedures to safeguard key generation and key management.

(b) Adopt internationally recognised standards and best practices to:

(i) establish secure mechanisms for the generation of keys, seeds, or other equivalent mechanisms. This includes considering all risks associated with the generation of a key or seed for a signatory.

(ii) encrypt and secure device storage for a customers' private keys when not in use. This includes ensuring that any keys stored online or in a single physical location are not capable of executing digital assets transactions, unless appropriate controls are in place.

(iii) store all key and seed backups in locations separate from the primary keys and seeds. Key and seed backups must be encrypted to a standard at least equivalent to that used to for the primary seed and key.

(iv) use a multi-signature arrangement, where appropriate. If a PSO adopts multi-signature arrangements that vary according to

transaction, it shall maintain well-documented procedures.

(c) Ensure that the employees involved in the key generation process are clearly identified and prevented from having unauthorised access to customers' digital assets.

10.3 Lost or stolen keys

(a) Establish and maintain effective policies and procedures to address situations where any keys or seeds of any digital assets wallet are lost, stolen or otherwise compromised, including but not limited to:

(i) recovery of affected digital assets;

(ii) ensure timely communication with all clients and counterparties regarding consequences arising from the relevant incidents, and the measures being taken to remedy such consequences;

(iii) cooperation with law enforcement agencies and regulatory bodies; and

(iv) wind-down arrangements and public disclosure of such arrangements, if applicable.

Question 6
Do you have any comments on the digital assets wallet management requirements? If yes, please provide your recommendation and justification.

11.0 Business Conduct

The PSO shall:

11.1 Act in the best interests of customers and take all reasonable measures to avoid situations that may give rise to conflict of interest with customers.

11.2 Safeguard the rights and interests of customers including ensuring that customers have continuous access to their funds and securities including digital assets and prevent any unauthorised access.

11.3 Ensure that all fees and charges payable are fair, reasonable and transparent.

11.4 Establish effective BCM including Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for all critical business functions to ensure the continuity of operations and timely recovery in the event of contingencies.

11.5 Establish and maintain written policies and procedures to:

(a) provide clear lines of reporting, authorisation and ensure proper segregation of functions;

(b) implement controls to prevent unauthorised access or fraudulent transactions;

(c) enable full disclosure to customers of all their transactions and assets;

(d) manage customers' data including the collection, storage, use, disclosure and disposal of customer information, including the following:

(i) proper handling and safeguarding of customer data;

(ii) protection of confidentiality and security of customer data; and

(iii) management of third-party service providers that have access to customer data.

(e) ensure that its processes and practices are continuously aligned with industry's best practices, including those relating to the safekeeping and administration of digital assets;

(f) ensure fair treatment of customers;

(g) identifies, monitors, mitigates and manages situations, including potential situations that may give rise to conflicts of interest;

(h) mitigate any potential losses in the event of any systems error, failure or malfunction; and

(i) govern customer's access to and withdraw their digital assets including, but not limited to, during periods of heightened uncertainty and/or extreme volatility.

11.6 Provide Labuan FSA with access to any register required to be maintained under the Guidelines and disclose any other information as may be required by Labuan FSA from time to time.

Question 7
Do you have any comments on the business conduct requirements? If yes, please provide your recommendation and justification.

12.0 Operational Requirements

12.1 Have and maintain at all times, a minimum paid-up capital that is unimpaired by losses as follows:

(b) RM1,000,000 for undertaking activities under paragraph 7.1 only; or

(c) RM1,500,000 for undertaking activities under both paragraphs 7.1 and 7.2.

In assessing an applicant's financial resources, Labuan FSA will consider the quality and quantity of the resources as well as their availability to the applicant. Labuan FSA may also exercise its discretion to require additional capital to commensurate with the business operations of the Labuan PSO, taking into account the risk profile as well as nature, scale, complexity and diversity of their business activities.

12.2 Conduct periodic reviews, audits and testing of its systems, operational policies, procedures, and controls and shall periodically report to the board and senior management on the assessment of material risks affecting the PSO, to ensure that such risks are managed and mitigated in a timely manner.

12.3 Appoint a Labuan approved auditor to carry out an annual audit of its accounts in respect of the business operations pursuant to LFSSA and LIFSSA that is fit and proper.

12.4 Obtain prior approval from Labuan FSA on the following matters:

(a) change of shareholding[6];

(b) appointment and change of its directors and principal officer;

(c) establishment of any office or subsidiary outside Labuan;

(d) outsourcing arrangement; or

(e) change of name.

12.5 Immediately notify Labuan FSA:

(a) of any breach of the terms and conditions imposed by Labuan FSA, or any provisions of the laws and regulatory requirements;

[6] For branch set-ups, only notification to Labuan FSA is required for the change of shareholding structure and appointment of its board of directors.

(b) when it becomes aware of any matter that adversely affects or is likely to adversely affect, its ability to meet its obligations under the Guidelines; and

(c) of the occurrence of any event which would trigger the activation or execution of the BCM.

12.6 Notify Labuan FSA within 7 days pertaining to the following matters:

(a) change of bank account where the paid-up capital has been deposited;

(b) resignation of directors or principal officer;

(c) change of place of business or office in or outside of Labuan;

(d) change to its constituent documents;

(e) significant event that affects its going concern or reputation; or

(f) change of its financial year end.

12.7 Maintain an operational office in Labuan. The operational office should be used for business purposes only and must be appropriately furnished with office equipment.

12.8 Ensure that the persons in control, directors and principal officer are fit and proper person, at all times, in line with the Guidelines on Fit and Proper Requirements issued by Labuan FSA.

12.9 Ensure compliance with the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 and the Guidelines on Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions (AML/CFT and TFS for Labuan KRIs) including any AML/CFT policy documents applicable to PSO.

12.10 Maintain adequate and proper records and books of accounts, transactions and fund flows, in Labuan that will sufficiently explain its transaction and financial position as required by the Directive on Accounts and Record-keeping Requirement for Labuan Entities issued by Labuan FSA. Its name and company number must be clearly indicated on its letterhead, stationery, and other documents.

12.11 Comply with applicable laws, rules and regulations relevant to the business including relevant guidelines issued by Labuan FSA, regulatory requirements of the jurisdictions where the PSO operate in, at all times. In this regard, it is expected to obtain all necessary approvals from the relevant authorities in the markets in which it intends to operate, including approvals for any promotional activities, where applicable, prior to commencing its business in those markets. A copy of such approvals shall be provided to Labuan FSA, where available or relevant.

Question 8
Do you have any comments on the operational requirements? If yes, please provide your recommendation and justification.

13.0 Reporting Requirement

13.1 Labuan PSOs are required to submit to Labuan FSA the following:

(a) audited financial statements via Supervisory Intelligent System (SIS) within six (6) months after the closure of each financial year: and

(b) statistics and any information as Labuan FSA may require from time to time.

14.0 Annual Fee

14.1 The annual fee payable is as specified under the *Labuan Financial Services and Securities (Amendment) Regulations 2022*.

14.2 The subsequent payment of annual licence fee is payable by 15 January of each year.

15.0 Application Requirements

15.1 Submit a duly completed application form with the relevant supporting documents as stipulated in the specified form that will be issued by Labuan FSA together with a processing fee as prescribed under the *Labuan Financial Services Authority (Processing and Approval Fees) (Labuan Financial Institutions) (Amendment) Order* 2022 or such amended or revised regulations as may be prescribed or advised by the Authority from time to time. The applicant may also opt for fast-track processing with additional fee [7].

[7] Subject to the Authority's acceptance of fast-track application.

15.2 Additionally, the applicant must submit a soft copy in PDF format of the completed application form and supporting documents together with the official receipt issued by Labuan FSA on the payment of processing fee.

15.3 Labuan FSA may require from the applicant such other information or documents for the purpose of determining the merits of the application.

16.0 Submission of Application and Enquiries

16.1 The application for approval and notification can be submitted to:

Head of Authorisation and Licensing Unit
Labuan Financial Services Authority
17th Floor, Main Office Tower
Financial Park Complex, Jalan Merdeka
87000 Federal Territory of Labuan, Malaysia.

16.2 Any enquiries or clarification may be directed at the following contact details:

Telephone no. : 03-8873 2000
E-mail : bpu@labuanfsa.gov.my (Guidelines)
bplicensing@labuanfsa.gov.my (Application)

Labuan Financial Services Authority
3 February 2026 (Exposure Draft)

Appendix I

List of Relevant Guidelines, Circulars and Directives

The following are the list of Guidelines/Circulars/Directives that are applicable to Labuan PSO:

1. Guidelines on Compliance Function for Labuan Financial Institutions
2. Guidelines on Market Conduct for Labuan Digital Financial Intermediaries
3. Guidelines on Technology Management
4. Guidelines on Digital Governance Framework
5. Guidelines on Market Conduct for Labuan Digital Financial Intermediaries
6. Guidelines on Travel Rule for Labuan Digital Financial Services
7. Directive on Financial Reporting Standards for Labuan Financial Institutions
8. Circular on Financial Reporting Standards for Labuan Financial Institutions
9. Directive on Accounts and Record-Keeping Requirement for Labuan Entities
10. Labuan International Business and Financial Centre Sustainability Taxonomy (LiST)

Disclaimer: The above lists are not exhaustive. In the event of any amendments to the existing guidelines, the stipulations outlined in the new/updated guidelines will prevail.