BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Electronic Know-Your-Customer (e-KYC)

Applicable to:
1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed life insurers
5. Licensed family takaful operators
6. Prescribed development financial institutions
7. Licensed money services businesses
8. Approved issuers of designated payment instruments and designated Islamic payment instruments

Issued on: 15 April 2024 BNM/RH/PD 030-16

TABLE OF CONTENTS

Part A Overview 1

1 Introduction 1
2 Applicability 1
3 Legal provisions 1
4 Effective date 2
5 Interpretation 2
6 Related legal instruments and policy documents 4
7 Policy documents superseded 5

PART B POLICY REQUIREMENTS 6

8 e-KYC implementation 6
9 Reporting requirements 12

PART C REGULATORY PROCESS 13

10 Notification for licensed persons and prescribed development financial institutions 13
11 Approval for licensed money services businesses 14
12 Enforcement 14

APPENDICES 15

Appendix 1: Examples of verification methods to establish business legitimacy 15
Appendix 2: False Acceptance Rate and sampling 16
Appendix 3: Minimum scope and criteria for external independent assessment 20
Appendix 4: e-KYC safeguards to be adopted by financial institutions offering higher risk financial products 24
Appendix 5: Information required for submission 27
Appendix 6: Submission instructions 28

PART A OVERVIEW

1 Introduction

1.1 Supported by further technological advancements and introduction of electronic Know-Your-Customer (e-KYC) solutions for the financial sector, digitalisation of the customer identification and verification processes has become an increasingly prominent enabler in the onboarding process for financial services.

1.2 Growing adoption and understanding of e-KYC solutions in the financial sector call for enhancements to existing requirements to ensure e-KYC solutions continue to remain relevant, robust and reliable. This includes expanding the scope of e-KYC applications to cover both individuals and legal persons, providing guidance on e-KYC solutions that can cater to the unbanked, while ensuring uncompromised accuracy in customer identification and verification.

1.3 This document sets out the minimum requirements and standards that a financial institution, as defined in paragraph 5.2, must observe in implementing e-KYC for the on-boarding of individuals and legal persons. The requirements outlined in this policy document are aimed at -

(i) Enabling safe and secure application of e-KYC technology in the financial sector;
(ii) Facilitating Bank Negara Malaysia's (the Bank's) continued ability to carry out effective supervisory oversight of financial institutions; and
(iii) Ensuring effective anti-money laundering, countering financing of terrorism and countering proliferation financing (AML/CFT/CPF) control measures.

2 Applicability

2.1 This document is applicable to all financial institutions as defined in paragraph 5.2 and any other institution that may be specified by the Bank.

2.2 This policy document shall not apply to agent banking channels governed under the Agent Banking Policy Document dated 30 June 2022.

3 Legal provisions

3.1 This policy document is issued pursuant to-

(i) sections 47(1) and 261(1) of the Financial Services Act 2013 (FSA);
(ii) sections 57(1) and 272 of the Islamic Financial Services Act 2013 (IFSA);
(iii) sections 41(1),126 and 123A of the Development Financial Institutions Act 2002 (DFIA);
(iv) sections 74 of the Money Services Business Act 2011 (MSBA); and
(v) sections 16 and 83 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA).

4 Effective date

4.1 This Policy Document comes into effect on 15 April 2024.

5 Interpretation

5.1 The terms and expressions in this Policy Document shall have the same meaning assigned to them in the FSA, IFSA, DFIA, AMLA and MSBA unless otherwise stated.

5.2 For the purposes of this Policy Document-

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action.

"**G"** denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted.

"authorised person" in the context of a business relationship with a financial institution, refers to a natural person appointed in writing[1] by a legal person to operate and maintain an account with a financial institution including to open, close and give any instruction for the conduct of financial transactions in the account on behalf of the legal person.

"**beneficial owner"** in the context of a legal person, refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person.

Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.

In insurance and takaful sectors, this also refers to any natural person(s) who ultimately owns or controls a beneficiary, as specified in the Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT/CPF and TFS for FIs) policy document.

"biometric" refers to a unique physical feature of a person based on a certain aspect of the person's biology. These include facial features, fingerprints or retinal patterns.

[1] By means of a letter of authority or directors' resolution or by electronic means, as permitted under the legal person's constitution. For avoidance of doubt, requirements relating to such electronic means can be referred in paragraph 8.16 of this policy document.

"Board" in relation to a company, refers to-
(i) directors of the company who number not less than the required quorum acting as a board of directors; or
(ii) if the company has only one director, that director.

"customer" refers to both account holder and non-account holder. The term also refers to a client.

For the life insurance and family takaful sector, "customer" refers to parties related to an insurance/takaful contract including potential parties such as the proposer/policyholder/policy owner, payor, assignee and company representative, but does not include insurance agent.

In the case of group policies, "customer" refers to the master policy holder, that is, the owner of the master policy issued or intended to be issued.

In addition, for money services business and designated payment instruments, "customer" refers to a person for whom the licensee or approved issuer of designated payment instruments undertakes or intends to undertake business relations.

Where the term "customer" is broadly used in this policy document, requirements shall apply to both individual and legal person.

"electronic Know-Your-Customer (e-KYC)" means establishing business relationships and conducting customer due diligence (CDD) [2] by way of electronic means, including online channel and mobile channels.

"financial institution" refers to-
(i) a licensed bank, investment bank and life insurer under the FSA;
(ii) a licensed Islamic bank and licensed family takaful operator under the IFSA;
(iii) a prescribed development financial institution under the DFIA;
(iv) an approved issuer of designated payment instruments under the FSA;
(v) an approved issuer of designated Islamic payment instruments under the IFSA; and
(vi) a licensed money services business under the MSBA.

"False Negative" refers to identification and verification cases processed under e-KYC solutions in which the solution falsely rejected and did not verify an identity when it should have been accepted. These include cases of genuine identities or documents that were falsely rejected.

[2] This includes the cases of standard and simplified CDD on individuals, legal persons and beneficiaries as specified under the AML/CFT/CPF and TFS for FIs policy document.

"False Positive" refers to identification and verification cases processed under e-KYC solutions in which the solution accepted and verified an identity when said identity should have been rejected. These include cases of false or unclear identities, forged or tampered documents and unclear images that were falsely accepted.

"individual" refers to a natural person.

"legal person" means a legal person as specified under paragraph 6.2 of the AML/CFT/CPF and TFS for FIs policy document. It refers to any entity other than a natural person that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, government-linked companies (GLC), foundations, partnerships, or associations and other similar entities.

GLC refers to an entity where the government is the majority shareholder or single largest shareholder and/or has the ability to exercise and influence major decisions such as appointment of board members and senior management.

"the Bank" means Bank Negara Malaysia.

"True Positive" refers to identification and verification cases processed under e-KYC solutions in which the solution rightly accepted and verified an identity. These include cases of genuine identities or documents that were rightly accepted.

"True Negative" refers to identification and verification cases processed under e-KYC solutions in which the solution rightly rejected and did not verify an identity. These include cases of false or unclear identities, forged or tampered documents and unclear images that were rightly rejected:

6 Related legal instruments and policy documents

6.1 Where applicable, this policy document must be read together with any relevant legal instruments, policy documents, guidelines, circulars, and supplementary documents issued by the Bank, in particular -

(i) Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT/CPF and TFS for FIs) policy document issued on 5 February 2024;
(ii) Risk Management in Technology (RMiT) dated 1 June 2023;
(iii) Outsourcing dated 23 October 2019;
(iv) Management of Customer Information and Permitted Disclosures dated 3 April 2023;
(v) Introduction of New Products dated 7 March 2014; and
(vi) Introduction of New Products by Insurers and Takaful Operators dated 15 May 2015.

6.2 For avoidance of doubt, where a financial institution is subjected to more than one policy document relating to e-KYC or non-face-to-face (FTF) requirements, the more stringent requirement shall apply.

7 Policy documents superseded

7.1 This policy document supersedes the Electronic Know-Your-Customer (e-KYC) policy document issued on 30 June 2020.

PART B POLICY REQUIREMENTS

8 e-KYC implementation

Role and responsibility of the Board

S 8.1 A financial institution shall obtain Board approval on the overall risk appetite and internal framework governing the implementation of e-KYC for both individuals and legal persons. The framework shall address-

i. high risk or material risk scenarios that require subsequent Board approval;
ii. variations or exceptions to existing e-KYC related products or methods that require subsequent Board approval;
iii. internal processes, mitigating controls and triggers for escalation to the Board where there may be potential concern on the effectiveness of the e-KYC solution performance and related processes (e.g., change of technology provider, review of e-KYC results, sufficiency of reporting); and
iv. other instances that require Board approval.

S 8.2 The Board of financial institutions shall be responsible for ensuring satisfactory measures are undertaken by the financial institution such that an appropriate level of performance of the e-KYC solution is maintained at all times. Such responsibilities of the Board should include but are not limited to ensuring improvements are undertaken by the financial institution to enhance the e-KYC solution in a regular and timely manner, and that the Board is satisfied that the level of performance of the e-KYC solution does not undermine the integrity of the identification and verification process.

S 8.3 The Board of a financial institution shall set and ensure the effective implementation of appropriate policies and procedures to address any risks associated with the implementation of e-KYC. These include operational, information technology (IT) and money laundering, terrorism financing, proliferation financing (ML/TF/PF) and fraud risks.

Identification and verification (IDV) of customers through e-KYC

A. General requirements

S 8.4 In line with requirements under the AML/CFT/CPF and TFS for FIs policy document, a financial institution shall ensure and be able to demonstrate on a continuing basis that appropriate measures for the identification and verification of a customer's identity through e-KYC are secure and effective. Measures for identification and verification shall be proportionate to the risk dimensions of e-KYC.

G 8.5 In relation to paragraph 8.4, where reference is made to face-to-face processes, this should mainly serve as guidance on the minimum expected baseline.

S 8.6 For the money services business sector, in meeting requirements under paragraph 8.4 of this policy document, money services businesses shall also comply with IDV requirements for new customers when establishing business relationships through e-KYC under the AML/CFT/CPF and TFS for Financial Institutions Policy Document.

S 8.7 A financial institution shall adopt an appropriate combination of authentication factors when establishing measures to verify the identity of a customer being on-boarded through e-KYC. The strength and combination of the authentication factors shall be commensurate to the risks associated with inaccurate identification for a particular product or service.

G 8.8 In respect of paragraph 8.7, a financial institution may give regard to the key basic authentication factors, which namely and amongst others include:

(i) something the customer possesses (e.g. national identity document such as an identity card, registered mobile number, company's certificate of incorporation);

(ii) something the customer knows (e.g. PIN, personal information, transaction history); and

(iii) in the case of individuals, something the customer is (e.g. biometric characteristics).

An e-KYC solution that depends on more than one factor is typically more difficult to compromise than a single factor system.

S 8.9 In verifying the identity of an individual or beneficial owner under paragraphs 8.10 and 8.13 of this policy document and as required under the AML/CFT/CPF and TFS for FIs policy document, financial institutions shall:

(i) be satisfied with the identity of the individual or the beneficial owner through reliable and independent documentation, electronic data or any other measures that the financial institution deems necessary;

(ii) be satisfied with the veracity of information referred to in paragraph 8.9 (i) when verifying the identity of the individual or beneficial owner; and

(iii) ensure that documents, data or information collected is kept up-to-date and relevant.

B. IDV through e-KYC for individuals

G 8.10 In identifying and verifying an individual's identity through e-KYC as required under paragraph 8.4 of this policy document and the AML/CFT/CPF and TFS for FIs policy document, a financial institution may undertake measures, including but not limited to the following-

(i) *Document verification* – i.e., ensuring that the government issued ID to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms;

(ii) *Biometric matching* – i.e., verifying the customer against a government issued ID[3] by utilising biometric technology; and/or

[3] i.e, National Registration Identity Card (NRIC), passport, or any other official documents.

(iii) *Liveness detection* – i.e, ensuring the customer is a live subject and not an impersonator (e.g. through use of photos, videos, synthetic human face masks[4]) by utilising liveness detection.

S 8.11 For the money services business sector, in meeting requirements under paragraph 8.10 of this policy document, money services businesses shall also comply with IDV requirements for individuals under the AML/CFT/CPF and TFS for FIs Policy Document.

C. IDV through e-KYC for legal person[5]

G 8.12 A financial institution may implement e-KYC to identify and verify legal persons, subject to meeting the requirements in this policy document and the requirements for legal persons specified under the AML/CFT/CPF and TFS for FIs policy document[6] on CDD for legal persons.

S 8.13 When implementing e-KYC for legal persons, a financial institution shall have due regard to the areas listed as CDD requirements for legal persons in the AML/CFT/CPF and TFS for FIs Policy Document. This includes but are not limited to:

(i) identification and verification of a legal person as an entity to establish the existence of a legitimate business.

(ii) identification and verification of the authorised person appointed by the legal person to establish business relations and conduct transactions on behalf of the legal person; and

(iii) identification and reasonable measures for verification of beneficial owners[7] of the legal person.

G 8.14 In relation to paragraph 8.13 (i), financial institutions may wish to undertake one or more verification methods to establish business legitimacy, such as but not limited to those specified under Appendix 1.

S 8.15 For the money services business sector, in meeting requirements under paragraph 8.13 (i) - (ii) and paragraph 8.14 of this policy document, money services businesses shall also comply with IDV requirements for legal persons, i.e., corporate customers and the authorised person under the AML/CFT/CPF/CPF and TFS for FIs Policy Document, as may be amended by the Bank from time to time.

---

[4] Synthetic human face masks are designed to impersonate real human faces and made from materials such as silicone or otherwise. For purposes of e-KYC, such masks may be used to defraud facial recognition software.

[5] For avoidance of doubt, a sole proprietor is not deemed as legal person under this policy document. Accordingly, the on-boarding of sole proprietors through e-KYC is subject to e-KYC process for individual as specified under paragraph 8.10.

[6] In particular, requirements relating to legal persons as well as clubs, societies and charities contained within paragraphs 14A.9, 14B.11, 14C.10 and 14D.9 of the AML/CFT/CPF and TFs for FIs Policy Document.

[7] As required under paragraphs 14A.9.6, 14B.11.12, 14C.10.7 and 14D.9.6 of the AML/CFT/CPF and TFS for FIs policy document.

S 8.16 In relation to paragraph 8.13 (ii), where the identification and verification of the authorised person is conducted via electronic means, a financial institution shall ensure that –

(i) electronic communication or documents that capture collective decision making by the directors of the legal person (e.g. digital forms of Directors Resolution or Letter of Authority) to appoint the authorised person and establish business relations are maintained in accordance with relevant record keeping requirements as specified under paragraph 24 of the AML/CFT/CPF and TFS for FIs Policy Document;

(ii) such electronic means adopted to identify and verify the authorised person are within the legal person's constitution or any other document which sets out the powers of the legal person; and

(iii) the authorised person is identified and verified through e-KYC as an individual, having due regard to the measures listed under paragraph 8.10 of this policy document.

G 8.17 In respect of paragraph 8.16 (i), such electronic means to capture collective decision making by the directors of the legal person on the appointment of the authorised person may include but are not limited to the following:

(i) utilising electronic technologies that identify and verify the directors, and subsequently capture evidence of directors' consent (e.g. audited/circulated email trails, providing agreement or disagreement through personal secure authentication links for directors to consent, video-conferencing to verify consent, digital signatures, use of secure electronic voting platforms, etc); and/or

(ii) using third parties (e.g. Digital Company Secretaries) that may provide confirmation on the legitimacy of relevant evidence such as the Directors Resolution or Letter of Authority.

S 8.18 A financial institution shall undertake their own risk assessment to clearly define parameters for classifying potential legal persons that are not allowed to establish business relations through e-KYC.

Ensuring effective e-KYC implementation

G 8.19 e-KYC solutions may utilise artificial intelligence, machine learning or other forms of predictive algorithms to ensure accurate identification and verification. This may result in automation of the decision-making process for customer on-boarding, thus reducing the need for human intervention.

S 8.20 Where the decision to verify a customer's identity through e-KYC is automated with the use of artificial intelligence, machine learning or other forms of predictive algorithms, whether in whole or in part, a financial institution shall ensure that the e-KYC solution is continuously capable of accurately distinguishing between genuine and non-genuine cases of customer on-boarding.

S 8.21 For the purposes of paragraph 8.20, in ensuring accuracy of the e-KYC solution, a financial institution shall take steps to minimise the False Acceptance Rates (FAR), defined as $\frac{False\ Positive}{(False\ Positive + True\ Negative)}\ x\ 100$. In measuring and assessing the FAR, a financial institution shall observe the considerations and requirements listed in Appendix 2[8].

S 8.22 Financial institutions shall ensure that the technology provider appointed to provide the e-KYC solution conducts the following:

(i) Ensure that the e-KYC solution, encompassing the three (3) e-KYC modules namely document verification, biometric matching and liveness detection as referenced in paragraph 8.10, has been assessed by a credible[9] external independent assessor in accordance with the scope and criteria as provided in Appendix 3. This includes ensuring that the technology provider has put measures in place to address the gaps or weaknesses identified from such assessment in a timely manner;

(ii) Ensure that the relevant certification(s) is obtained for the various modules under e-KYC solution, where such certification is available[10].

S 8.23 Financial institutions that have yet to implement e-KYC (i.e. first-time implementation) or wish to change the e-KYC solution or technology provider used are required to ensure the following:

(i) Financial institutions must perform due diligence on the identified technology provider and the e-KYC solution. The due diligence, which must be validated by an independent party, shall include the following:

a. Assessment whether the technology provider has a good track record, experience and expertise in offering solutions involving regulated entities and products; and

b. Assessment of the e-KYC solution's technical capabilities (e.g. parameters, methodology of models used).

(ii) Prior to implementing the e-KYC solution, financial institutions shall fulfil the requirements in paragraph 8.22[11].

S 8.24 Financial institutions shall review or revalidate requirements under paragraph 8.22 for continued relevance at least once every three (3) years, or where there are any material changes to the e-KYC solution.

---

[8] For avoidance of doubt, requirements for FAR within this policy document do not apply to e-KYC solutions where verification of customer identity is automated without the use of artificial intelligence, machine learning or other similar forms of predictive algorithms.

[9] Credible external independent assessor refers to an assessor who has the capability and expertise in conducting assessments on identity verification solutions.

[10] The modules are biometric matching/facial recognition, liveness test and ID verification. For example, ISO 19794-5 for facial recognition and ISO 30107-3 for liveness test (presentation attack detection) module.

[11] This requirement must be completed prior to implementation of the e-KYC solution unless:

(i) Such assessment has already been conducted by the technology provider within the past two (2) years; or

(ii) Where the technology provider has experience in applying the e-KYC solution effectively for other financial institutions and has established a good track record, this requirement may be completed no later than one (1) year from the date of the financial institution's e-KYC implementation.

S 8.25 Notwithstanding requirements under paragraphs 8.22 and 8.23, to ensure an effective overall implementation of e-KYC, financial institutions shall conduct an independent assessment on the financial institution's own processes, procedures and controls prior to first-time implementation of an e-KYC solution and undertake a review of the independent assessment on a regular basis, as may be determined by the financial institution based on its own risk assessment.

Reliance on human representatives

G 8.26 Notwithstanding paragraphs 8.19 to 8.21, a financial institution may also perform e-KYC where identification and verification is conducted solely by a human representative. This includes cases where the decision to verify a customer is conducted by a financial institution representative, intermediary or insurance agent, with the assistance of electronic means such as video calls using mobile devices.

G 8.27 In contrast with e-KYC solutions under paragraphs 8.19 to 8.21 that utilise both machine and human [12] capabilities, e-KYC performed solely by a human representative through electronic means may involve a lower level of identity assurance due to human limitations and thus may not be suitable for all circumstances.

S 8.28 Where the decision to verify a customer's identity through e-KYC is conducted solely by a human representative, a financial institution shall give due regard to situations where there is potential for higher risk of misidentification and establish internal safeguard measures to address this risk.

Addressing ongoing vulnerabilities

S 8.29 A financial institution shall continuously monitor, identify and address potential vulnerabilities[13] in the e-KYC solution. Where potential vulnerabilities in the e-KYC solution are detected, a financial institution shall identify and adopt immediate mitigation measures as necessary, including for higher risk products.

S 8.30 In respect of paragraph 8.29, actions to address potential vulnerabilities shall include:

(i) Conducting reviews on the e-KYC solution and, where applicable, submitting periodical feedback to technology providers with the aim of improving effectiveness of the underlying technology used for customer identification and verification; and

(ii) Risk considerations, trigger mechanisms and rectification measures as listed in Appendix 2.

[12] By virtue of audits that are conducted under Appendix 2.

[13] Potential vulnerabilities include exposures to IT, operational and ML/TF/PF related risks.

Additional safeguards to facilitate deployment

G 8.31 The availability of data is an important factor in the effectiveness of e-KYC solutions for identification and verification.

S 8.32 Where there are limited data points to determine accuracy of the e-KYC solution in the initial deployment stage, a financial institution shall implement additional safeguards, particularly for products that pose higher risks arising from inaccurate identification.

S 8.33 To facilitate deployment of e-KYC solutions for products with higher risks arising from inaccurate identification, a financial institution shall observe the considerations and safeguards specified in Appendix 4. This list may be specified, amended or superseded from time to time as and when there are developments in the e-KYC landscape, including availability of better performance data on the effectiveness of specific e-KYC methods.

9 Reporting requirements

S 9.1 In monitoring the effectiveness and accuracy of e-KYC solutions utilising artificial intelligence, machine learning or other forms of predictive algorithms, a financial institution shall maintain a record of the performance of the e-KYC solution segregated on a monthly basis.

S 9.2 The records required to be maintained under this policy document shall be made readily available for review by the Bank.

S 9.3 A financial institution shall submit the record in relation to paragraph 9.1 via the STATsmart Integrated Submission Platform (ISP) accessible via Kijang.Net (refer to Appendix 6 for details).

S 9.4 A financial institution shall submit the record in relation to paragraph 9.1 on a half-yearly basis according to the following arrangement-

(i) For the period of January to June of each year, the record shall be submitted no later than 4 August of the same year; and

(ii) For the period of July to December each year, the record shall be submitted no later than 4 February the following year.

S 9.5 In respect of paragraph 9.4, in the event that the deadline falls on a non-working day, the deadline will be extended to the next immediate working day, unless specifically informed by the Bank in writing on the revised deadline.

PART C REGULATORY PROCESS

10 Notification for licensed persons and prescribed development financial institutions

S 10.1 Subject to paragraphs 8.1 and 8.3, where a licensed person[14] or a prescribed development financial institution[15] meets the requirements stipulated in this policy document and intends to implement an e-KYC solution described in paragraph 8.19 for the first time[16] or change the appointed technology provider for the e-KYC solution, a complete list of information as set out in Appendix 5 shall be submitted to the Bank. This shall also include a complete list of information to demonstrate that the technology provider complies with requirements set out in paragraph 8.22 and Appendix 3 of this policy document.

S 10.2 In respect of paragraph 10.1, a licensed person or a prescribed development financial institution may proceed to implement and utilise the e-KYC solution after 14 working days from the date of receipt by the relevant Departments of the Bank of the complete submission of information set out in Appendix 5. The submission of information to the Bank shall be made to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be and shall be signed off by the Chief Executive Officer, Chief Risk Officer or Chief Operating Officer who has the responsibility to ensure that the information submitted pursuant to this paragraph is complete and accurate.

G 10.3 In respect of paragraph 10.1, where a licensed person or a prescribed development financial institution intends to implement the e-KYC solution for the first time and the product to be offered qualifies as a new product as defined under the Introduction of New Products policy document[17], the information required under the aforementioned policy document and this policy document may be submitted together to the Bank.

S 10.4 Prior to submitting the information required in paragraph 10.1, a licensed person or a prescribed development financial institution, shall ensure, where relevant, approvals such as those in relation to the Bank's RMiT and Outsourcing policy documents are obtained.

---

[14] As defined under the FSA or IFSA.
[15] As defined under the DFIA. This excludes cases where a prescribed development financial institution licensed under the MSBA intends to implement e-KYC for remittance services.
[16] For avoidance of doubt, this requirement also applies to a financial institution implementing e-KYC in the following situations for the first time: (i) e-KYC for legal persons; and/or (ii) e-KYC for higher risk products without a credit transfer safeguard.
[17] Or in the case of life insurers and family takaful operators, the Introduction of New Products by Insurers and Takaful Operators policy document.

11 Approval for licensed money services business

S 11.1 Subject to paragraphs 8.1 to 8.3 and as required under the AML/CFT/CPF and TFS for FIs policy document, licensed money-changing operators, licensed remittance service providers[18], approved non-bank issuers of designated payment instruments and approved non-bank issuers of designated Islamic payment instruments shall obtain a written approval from Jabatan Pemantauan Perkhidmatan Pembayaran prior to implementing e-KYC or changing the appointed technology provider for the e-KYC solution.

S 11.2 In respect of paragraph, 11.1, application for approval shall include a complete list of information as set out in Appendix 5 and a complete list of information to demonstrate that the technology provider complies with requirements set out in paragraph 8.22 and Appendix 3 of this policy document.

12 Enforcement

12.1 Where the Bank deems that the requirements in this document have not been complied with, the Bank may take appropriate enforcement action against the financial institution, including the directors, officers and employees with any provision marked as "S" in this document or direct a financial institution to-

(i) undertake corrective action to address any identified shortcomings; and/or

(ii) suspend or discontinue implementation of e-KYC.

[18] This includes cases where a prescribed development financial institution licensed to conduct remittance service under the Money Services Business Act 2011 (MSBA) intends to implement e-KYC for remittance services.

APPENDICES

Appendix 1: Examples of verification methods to establish business legitimacy

1. In developing e-KYC methods for legal persons, a financial institution may wish to consider undertaking at least one or more verification methods that is relevant to the nature or business model of the legal person. This aims to provide heightened assurance on the legitimacy of the legal person's business.

2. Such verification measures may include but not be limited to the following:

   (i) make video calls to the CEO, directors, or authorised person assigned to the legal person. During the video call, reporting institutions may request the person to show proof of business existence such as signboard or inventories (if any). During the video call, a financial institution may request the person to show proof of business existence such as signboard or inventories (if any). A financial institution may consider making unannounced video calls depending on the ML/TF/PF risk identified on a particular customer. Such unannounced call may be effective in identifying circumstances where a fraudulent business had staged its premise in advance of the call;

   (ii) identify and verify the location of legal person to ensure that the location matches the registered or business address of the legal person via methods that provide high levels of assurance and are legally permissible[19]. A financial institution may also verify location of the CEO, directors, or authorised person during the video call;

   (iii) verify the legal person's information against a database maintained by credible independent sources such as relevant regulatory authorities, government agencies or associations of the regulated sectors. A financial institution may also request for the legal person's active bank account statement or audited financial statement as proof of on-going business activity; and/or

   (iv) any other credible verification methods as proposed by financial institutions to the Bank.

[19] Examples of such methods include (but are not limited to) video calls, use of internet map/location services, drones, or visits by the financial institution's agent network.

Appendix 2: False Acceptance Rate and sampling

1. In measuring the accuracy and effectiveness of e-KYC solutions, the FAR may be considered a useful measurement as it captures the capability of the solution to identify non-genuine identification and verification cases. Generally, a lower FAR indicates that the e-KYC solution has correctly identified non-genuine or fraudulent identification and verification attempts on a regular basis.

2. FAR shall be measured based on the number of complete[20] identification and verification cases processed under e-KYC.

3. In determining FAR, a financial institution shall conduct audits to classify identification and verification cases into genuine and non-genuine cases. Where it is not feasible for a financial institution to audit every identification and verification case facilitated through e-KYC, a financial institution may adopt a sampling approach. In doing so, a financial institution shall adopt a risk-based sampling approach in determining the appropriate sample size for each module[21] of the e-KYC solution and ensure that the sample size data used to determine FAR is random, unbiased and representative of the entire population of customers.

4. In determining the appropriate sample size and group, a financial institution shall ensure that FAR calculations are based on total sample cases tested (i.e. if 1,000 cases were tested as the sample size, then the FAR data submitted must be based on the 1,000 cases sampled).

5. In determining the appropriate sampling approach, a financial institution shall at minimum take into consideration the following sampling dimensions to ensure that FAR results from the sample size tested appropriately reflects the severity of any FAR threshold breaches[22]:
   (i) *Minimum sample size*: The sample size shall minimally meet a 95% confidence level and 3% margin of error or 400 cases per month, whichever is higher.
   (ii) *Time-based considerations*: For the first 6 months of implementation where the level of assurance of the e-KYC solution effectiveness is not yet optimal, a higher sample size is recommended to gain a higher level of assurance. Subsequent to this, a financial institution may lower the sampling size tested if the FAR performance is satisfactory.
   (iii) *Risk-based considerations*: For higher risk financial products or segments (e.g. current and savings account for customers that do not have an existing bank account), a financial institution may wish to conduct a larger or full sampling approach.

[20] A complete identification and verification case processed under e-KYC is defined as a case where the customer has completed only the e-KYC checks as described in paragraph 3 of Appendix 4. This includes cases where e-KYC for individuals related to legal persons are implemented. This does not include other steps in the e-KYC process (e.g. credit transfer).
[21] i.e., facial recognition, liveness detection & ID document.
[22] For avoidance of doubt, the higher or stricter of considerations in (i) – (iv) shall apply in determining the minimum sample size. For example, if the minimum sample size required from 5(ii) is lower than that needed to meet requirements in 5(i), the minimum sample size required shall not be lower than that of 5(i).

(iv) *Progressive sampling*: Where one or more false positives are detected in the initial sample, a financial institution may wish to consider a higher sample size, with a focus on e-KYC cases that may share the same profile and result in a similar outcome as the identified false positive case.

6. A financial institution shall make readily available upon request by the Bank, information on false positive cases that are genuine fraud attempts and cases that were falsely accepted by the solution due to other reasons[23].

7. In respect of paragraph 3 of this Appendix, a financial institution shall conduct audits on current month e-KYC cases by the last day of the following month (e.g. January cases to be audited by the last day of February) for the first six months of e-KYC implementation. After the first six months of e-KYC implementation, a financial institution shall conduct the audits no less than once every quarter, where current quarter e-KYC cases shall be conducted by the last day of the first month of the following quarter (e.g. first quarter cases to be audited by the last day of April).

8. In principle, a financial institution is highly encouraged to strive to ensure that the overall FAR of the e-KYC solution is as low and close to zero as possible. Nevertheless, a financial institution should also take into consideration other data points beyond FAR to form an informed view of the risk level and effectiveness of the solution. This may include factors such as the number of identification and verification cases, number of false positives, availability of other safeguards, fraud patterns observed, and the risks associated with inaccurate identification for a particular product or service offered through e-KYC.

9. Generally, for e-KYC solutions leveraging the use of artificial intelligence, FAR should reduce with the increase in identification and verification cases processed.

10. To strengthen solution performance and enable quicker cadence for remedial action, a financial institution shall adopt a tiered approach for FAR threshold monitoring, review and notification, as follows:

Table 1: FAR thresholds and actions to be taken

FAR thresholds	Action to be taken when breached
Level 1 (0% – 3%)	A financial institution shall continuously monitor and improve the capability of e-KYC solutions.

[23] Reasons may include but are not limited to blurry images (ID images that are blurry but may be genuine, which were falsely accepted by the solution but should have been rejected), poor image quality, poor lighting or overexposure during facial recognition/ID document verification step, poor framing of the face/ID document, etc.

Level 2 (> 3%)	A financial institution shall conduct a risk assessment for notification to the Board and internal review to strengthen the e-KYC solution, including taking the appropriate rectification measures. In conducting the risk assessment, financial institutions may consider the FAR performance together with other relevant factors, observation points and considerations to provide an informed view of the risk level of the solution performance. For example, this may include the total number of identification and verification cases performed, number of false positives, existing mitigating controls, fraud patterns observed, etc.
Level 3 (> 5%)	Where FAR is measured to be more than 5% for any two months within a four-month period, a financial institution shall notify the Bank and submit an assessment of the e-KYC solution performance and mitigation measures. The notification shall be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan, Jabatan Penyeliaan Insurans dan Takaful or Jabatan Pemantauan Perkhidmatan Pembayaran, as the case may be, in writing within seven (7) working days upon the completion of the latest audit and detection of this FAR scenario.

11. In respect of paragraph 10 of this Appendix, the notification to the Bank shall include the following-
    (i) an assessment on the current performance of the e-KYC solution, including reasons for the observed level of FAR, risk level of the e-KYC solution, as well as existing mitigating controls in place;
    (ii) an assessment on whether the false positive case was successfully onboarded, or if the false positive case was detected and rejected through other mitigating controls[24] already in place as part of the e-KYC process. This assessment shall also include an analysis on the nature of the false positive cases (e.g. whether the cases are related to any mule activity, an emerging fraud trend/modus operandi, suspicious transactions, etc);
    (iii) proposed rectification actions to reduce the FAR going forward and address any identified vulnerabilities;
    (iv) proposed new mitigating actions or additional controls to safeguard the effectiveness of the e-KYC process; and
    (v) evidence that the Board is satisfied with items (i) to (iv) above, and with the decision to either continue or suspend using the same e-KYC solution, when such assessment by the Board has been made.

[24] e.g., Via verification against existing credible bureau files, fraud databases or any other form of fraud detection measures.

12. In respect of paragraph 11 (iv) of this Appendix, the mitigating actions and/or additional controls may include but are not limited to the following-
    (i) enhanced monitoring of customers identified and verified through e-KYC; and/or
    (ii) conducting audits on e-KYC cases prior to opening an account.

13. Where FAR exceeds 5% and the Bank assesses a financial institution and its Board did not effectively undertake the expected rectification measures on vulnerabilities that were identified, relevant enforcement action may be taken against the financial institution. The Bank may also specify controls or intervention measures as deemed necessary.

Appendix 3: Minimum scope and criteria for external independent assessment

Introduction

1. The AML/CFT/CPF & TFS for FI PD[25] requires reporting institutions to ensure the systems and technology deployed for the purpose of establishing a business relationship using non-face-to-face channels (including e-KYC) have the capabilities to support an effective AML/CFT/CPF compliance programme[26].

2. Hence, the objective of the external independent assessment in paragraph 8.18 of this policy document is to identify the overall effectiveness[27] and robustness of the e-KYC solution in detecting and mitigating ML/TF/PF and fraud risks at the point of customer on-boarding. The assessment shall include any identified gaps/weaknesses in the e-KYC solution, areas for improvement and recommendations to address such gaps/weaknesses.

Scope

3. The assessment shall cover the three (3) modules of an e-KYC solution, namely facial recognition, liveness detection (presentation attack detection) and Identity Document (ID) verification (which includes MyKad, international passports or any other common IDs used).

Criteria of assessment

4. The assessment shall be conducted in accordance with an appropriate methodology that is clear, structured and effective in delivering the intended objectives.

5. The assessment shall be conducted on a risk-based approach and shall ensure areas of higher risk are given an appropriate level of focus and intensity.

6. The assessment shall:
   (a) Determine whether the e-KYC solution fulfils the requirements in relevant established standards and practices, if any;
   (b) Evaluate effectiveness of the methodology and key parameters used in the relevant modules of the e-KYC solution, to the extent possible;

---

[25] Under paragraphs 14A.15.8 (for Banking and Deposit-Taking Institutions), 14.17.10 (for Insurance and Takaful), 14C.16.13 (for Money Services Business) and 14D.16.11 (for Non-Bank Issuers of Designated Payment Instruments and Designated Islamic Payment Instruments).

[26] As part of the AML/CFT/CPF compliance programme, under paragraph 14A.3 (for Banking and Deposit-Taking Institutions), 14B.3 (for Insurance and Takaful), 14C.4 (for Money Services Business) and 14D.3 (for Non-Bank Issuers of Designated Payment Instruments and Designated Islamic Payment Instruments), reporting institutions are required to conduct customer due diligence (CDD) to identify the customer and verify that the customer's identity using reliable, independent source document, data or information.

[27] Effectiveness is defined as the overall ability of the e-KYC solution to detect identity fraud and not deemed as indicating whether a particular e-KYC solution is being endorsed and/or more effective than others.

(c) Take into consideration any certifications[28] and tests results/outcome on the e-KYC solution by credible independent bodies[29]; and

(d) Ensure breakthrough testing is conducted in accordance with the minimum requirements under paragraph 7 of this Appendix.

7. Breakthrough testing are tests conducted on the e-KYC solution from end-to-end to mimic a malicious attacker. Specific requirements for breakthrough testing on the e-KYC solution are as follows:

(a) The tests shall be conducted in a comprehensive and effective manner, in line with emerging fraud techniques;

(b) The tests shall consist of various test scenarios for each module under the e-KYC solution, including the following as well as any other alternative but equally robust test scenarios:

Module	Test Scenarios

ID verification	• Physical tampering of ID.
	• Digital tampering of ID.
	• Use of fake ID:
	  ○ Low quality fakes (e.g., self-generated)
	  ○ Medium quality fakes (e.g., ID that may be produced by printing shops)
	  ○ If possible, use of high quality fakes.

Facial recognition	• Tampering of selfie image but not ID. • Tampering of ID but not selfie image. • Tampering of both selfie image and ID. • Use of different person's selfie vs ID (eg. Mr.A's selfie against Mr.B's ID)
Liveness test	Presentation attack detection test may be done in conformance to ISO/IEC 30107-3 standards, where there is increasing degree of sophistication as commercially available technology solution to produce biometric artefacts become more readily available. This shall include at minimum the following: • Use of simple artefacts produced with equipment readily available in a normal home e.g., 2D mask. • Use of 3D mask. • Use of falsified biometric traits e.g. facial image using software readily available in the market 'ShallowFake' application.

[28] Such as ISO 30107-3 on presentation attack detection and ISO 19794-5 on standardized face image format for facial recognition application.

[29] For example, for each module under the e-KYC solution, the assessment on the capability of the e-KYC solution should be made. This can be done by comparing any credible third-party independent test results (such as National Institute of Standards and Technology (NIST) Facial Recognition Vendor Test (FRVT), NIST FRVT Presentation Attack Detection (PAD) or National Fintech Evaluation Center (NFEC) facial recognition assessment), against a known benchmark (such as known accuracy for humans in facial matching capability).

	• If possible, use of falsified biometric traits created using artificial intelligence technology "DeepFake" application. • Coverage of the test scenarios must reflect the latest identity impersonation and cyber-attack techniques.

(c) The tests must be done using an adequate sample size in accordance with the various test scenarios for each module. The number of test samples should be risk-based (for instance, a smaller number of test samples can be prepared for a module that has undergone credible tests or met a known benchmarked, whereas more vigorous testing is required with higher sample size for a module which has not undergone any credible test or benchmark).

(d) Test samples shall be representative of and adequately reflect the demographics of an FI's customers (e.g., coverage of race, gender, age, etc).

(e) Test samples shall consist of low, medium and high quality of samples[30].

(f) The tests shall include replay attacks test (e.g., resubmission of identical images test, man-in-the-middle attack via network layer packet transmission approach), where at least two rounds of random re-tests shall be conducted.

(g) For ID verification, it is recommended that the testing include the elements below:

i. Detection of tampered personal data e.g. name, address
ii. Detection and verification of micro print (e.g., existence and features of micro print, font type and size, unique colour);
iii. Detection and verification of hologram image (i.e., comparison of hologram image against ID image and selfie);
iv. Official markings (e.g., the Malaysian flag, MyKad logo, font type and size)
v. Identity card number (e.g., consistency of presented MyKad with existing numbering and format conventions, for passport the machine-readable zone (MRZ) bit-check number and format conventions); and

(h) ID verification shall include verification of passports that are compliant with International Civil Aviation Organisation (ICAO) standards. The ID verification on international passports shall focus more on passports from countries where the financial institution's customers are commonly from.

[30] For example, low quality test samples are simple, fast and cheap to produce. Medium quality test samples are moderately difficult to produce, takes longer time (eg.1-3 days) and involves moderate investment. Where else high quality test samples are generally difficult/requires more expertise to produce, takes longer time and can be expensive.

8. The outcome of the assessment shall be adequately and clearly documented and shall be submitted to the TPs and subsequently submitted to the relevant financial institutions. The outcome of the assessment shall include the following:
    i. areas of gaps/weaknesses and areas for improvement; and
    ii. recommendations to address any weaknesses or gaps detected. This shall also include recommendation on any certifications required.

Appendix 4: e-KYC safeguards to be adopted by financial institutions offering higher risk financial products

1. List of products[31] subjected to e-KYC safeguards:
   (i) current account;
   (ii) savings account; and
   (iii) unrestricted investment account with funds placement and withdrawal flexibilities as well as funds transfer features.

e-KYC for individuals with credit transfer for higher risk products

2. A financial institution offering the financial products in paragraph 1 of this Appendix through e-KYC for the purpose of customer identification and verification shall at minimum-
   (i) verify the customer against a government issued ID by utilising biometric technology;
   (ii) ensure that the government issued ID used to support e-KYC customer verification is authentic by utilising appropriate fraud detection mechanisms;
   (iii) ensure the customer is a live subject and not an impersonator (e.g. use of photos, videos, synthetic human face masks) by utilising liveness detection; and
   (iv) undertake measures to demonstrate that the customer has an existing bank account with another licensed person and is able to access said bank account. This may be achieved through requiring the customer to perform a credit transfer or to verify an amount transferred to the said bank account.

3. In respect of paragraph 2 (iv) of this Appendix, a financial institution shall ensure that the customer details (i.e. name or identity document number) obtained in relation to the bank account with another licensed person is consistent with the details supplied by the customer.

4. In addition to requirements under paragraph 3 of this Appendix, a financial institution may also consider additional verification measures listed in paragraph 10 of this Appendix for higher levels of assurance, where deemed appropriate based on its own risk assessment.

e-KYC for individuals without credit transfer for higher risk products

6. The requirement in paragraph 2 (iv) of this Appendix does not apply where an individual customer does not have any existing bank account with another licensed person and thus is unable to perform the credit transfer step. In lieu of the credit transfer safeguard, a financial institution intending to offer the products listed in this Appendix to individual customers shall ensure to:
   (i) have in place sufficient controls based on internal assessment of risk arising from offering the product without the credit transfer step;

[31] Requirements in this Appendix apply to existing individual customers of a financial institution that do not have any of the products listed in paragraph 1 of this Appendix and is intending to apply for one through e-KYC.

(ii) be able to demonstrate that their e-KYC solution remains effective and secure;
(iii) build in a combination of both additional verification measures and ringfencing parameters to establish higher assurance levels and limit risk exposure; and
(iv) build in safeguards such that products offered in paragraph 1 of this Appendix to customers that do not have an existing bank account shall not have fund transfer capabilities to accounts of the same customer name.

7. In respect of paragraph 6 (iv) of this Appendix, this requirement may be waived subject to the following conditions:
   (i) Availability of and implementation of infrastructures that enable the accounts opened under paragraph 6 of this appendix to be clearly distinguished from other accounts under paragraph 1 of this appendix at all times; or
   (ii) Use of a trusted National Digital Identity[32] for identity verification.

8. In respect of accounts opened under paragraph 6 of this Appendix, a financial institution may, subject to their own risk assessment, consider uplifting ringfencing parameters imposed under paragraph 6 (iii) and fund transfer limitations under paragraph 6 (iv) where the financial institution ascertains the customer is genuine and determines the customer may be upgraded to full capability accounts, subject to the following conditions:
   (i) Sufficient account activity is observed for at least twelve months and the financial institution's satisfactory assessment [33] that the account is genuine; or
   (ii) The customer consents to visit a bank branch for physical identity verification.

9. In respect of paragraph 6 of this Appendix, a financial institution shall take reasonable measures to verify whether the individual customer has an existing bank account with another licensed person. This may include but are not limited to the following measures:
   (i) initiating an instant transfer (i.e. *DuitNow*) query via the customer's mobile phone number or IC number and verifying whether information on the query matches the customer's personal details or otherwise;
   (ii) presenting a declaration form for the customer to confirm that the customer does not have an existing bank account with another licensed person; or
   (iii) through any other credible methods or infrastructures as may be proposed for the Bank's consideration.

[32] Issued by the relevant authorities of the government of Malaysia.
[33] A financial institution's decision to graduate the account must be well documented.

10. In respect of paragraph 4 and paragraph 6 of this Appendix, examples of additional verification measures and ringfencing parameters that may be undertaken and built into the e-KYC process to provide a higher level of assurance for customers include but are not limited to:

Ringfencing parameters

(i) limiting product functions (e.g. lower account size and fund transfer limits, no cross-border wire transfer) at the initial period of account opening (i.e., at least 12 months post-account opening).

Additional verification measures

(i) performing a credit transfer from an existing e-wallet account held by the customer with a participating *DuitNow* e-wallet provider *(applicable to customers without an existing bank account with another financial institution only)*;
(ii) conducting audits for on-boarding cases prior to granting access to account;
(iii) telephone or video calls to the customer;
(iv) utilising device-based indicators to detect potential fraud attempts (e.g. consistency of IP address, geo-location, device IDs, methods to detect jailbroken/rooted devices and network connection used);
(v) analysing publicly available data (e.g. social media and digital footprints) to check for identity consistency;
(vi) requesting for official documents issued by government agencies or credible providers which can be verified by the document issuer (e.g. income statement, utility bills, etc);
(vii) requiring customers to complete online questionnaires for account opening applications that require a wide range of information, which can be verified;
(viii) confirming the customer's identity during physical delivery of bank cards;
(ix) introducing specific transaction monitoring scenarios/parameters and stricter on-going due diligence review cycles and triggers for accounts opened through e-KYC; and conducting randomised audits on e-KYC cases post on-boarding.

11. In relation to paragraph 8 of this Appendix, the financial institution's decision to graduate the account must be well documented and maintained in accordance with record keeping requirements under the AML/CFT/CPF and TFS for FIs policy document and must be made available to the Bank upon request.

Appendix 5: Information required for submission

1. A detailed product description, including its features, structure and target market or customers. Product illustrations shall also be included where appropriate.

2. Sample product term sheet.

3. Detailed information on the key features of the e-KYC solution. This may include types of checks, customer information captured and any other material information.

4. A written assessment on the effectiveness of the e-KYC solution. The written assessment may consider accuracy of technology functions, types of checks included and any other relevant information that may attest for the effectiveness of the underlying technology. Where relevant, the assessment should include FAR results gathered from conducting negative testing of fraudulent scenarios[34] on the e-KYC solution. Other relevant information supporting the written assessment such as independent assurance, review or certification may also be considered for this purpose.

5. In the case where a financial institution chooses to engage a technology provider, the assessment to demonstrate effectiveness of the e-KYC solution shall include a complete list of information to demonstrate that the technology provider complies with requirements set out in paragraph 8.22 and Appendix 3 of this policy document. The assessment may also include the technology provider's company background and track record in other jurisdictions or industries.

6. Description of key inherent risks of the e-KYC solution and arrangements in place to manage those risks. Where a financial institution deems it necessary, plans for implementation of enhanced monitoring and reporting mechanisms to identify potential ML/TF/PF activities should also be included in the description.

7. Detailed end-to-end process flow of the e-KYC solution. This may include but is not limited to an illustration of the customer journey and decision-making process from start of application to account opening.

8. Any other relevant information to demonstrate a financial institution's ability to comply with the standards in this document and any other related policy documents issued by the Bank, including, where applicable-
   (i) AML/CFT/CPF and TFS for FIs policy document;
   (ii) RMiT policy document;
   (iii) Electronic Money (E-Money) policy document;
   (iv) Governance, Risk Management, and Operations for Money Services Business (MSB) policy document; and
   (v) Outsourcing policy document.

9. Any additional documents or information as may be specified by the Bank.

[34] Negative testing may include testing the e-KYC solution against photocopied ICs, deepfake technology or any other method which may spoof the e-KYC solution into accepting an inaccurate on-boarding attempt.

Appendix 6: Submission instructions

1. The completed e-KYC reporting template shall be submitted to the Bank via the Integrated Submission Platform (ISP) on https://kijangnet.bnm.gov.my.

2. Please refer to the 'User Manual on Kijang.Net, Integrated Submission Platform and Entity Database for Reporting Entities' accessible here or via Kijang.Net Portal for guidance on the following:

   (i) Access to the Kijang.Net Portal
   (ii) User registration and approval process
   (iii) Submission process

   Enquiries on reporting-related matters shall be addressed to Jabatan Pengurusan Data dan Statistik (JPS) via email or telephone as specified below:

   (i) Group Email address : jps_ips@bnm.gov.my
   (ii) Telephone number : +603 26988044
   (iii) Extension : 7225, 7999, 7819, 7799