Guidelines on Electronic Know-Your-Customer (e-KYC)

Issuing Authority: Bank Negara Malaysia
Document No: BNM/RH/PD 030-10
Effective Date: 1 July 2024
Version: 1.2

> **Revision Notice:** This version supersedes version 1.1 dated 1 April 2024. Please refer to the revision history at the end of this document.

1. Introduction

This document sets out the regulatory expectations for financial institutions implementing electronic Know-Your-Customer (e-KYC) solutions for customer onboarding and ongoing due diligence. These guidelines apply to all licensed banks, Islamic banks, insurers, and prescribed institutions under the purview of Bank Negara Malaysia.

Financial institutions are expected to adopt robust technology solutions that balance customer convenience with the integrity of verification processes. The adoption of e-KYC shall not compromise the quality of customer due diligence conducted by the institution.

2. Scope of Application

These guidelines are applicable to the following categories of financial institutions:

1. Licensed banks and licensed Islamic banks
2. Licensed insurers and licensed takaful operators
3. Prescribed institutions under the Development Financial Institutions Act 2002
4. Payment system operators and e-money issuers

3. Minimum Requirements for e-KYC Technology

3.1 Identity Verification

All e-KYC solutions must incorporate the following minimum capabilities for identity verification:

Component	Requirement	Standard
Document Authentication	Verify authenticity of identity documents (MyKad, passport)	ISO/IEC 19794-5
Facial Recognition	Liveness detection with anti-spoofing measures	ISO/IEC 30107-3 Level 1
Data Extraction	Automated extraction of personal data from identity documents	ICAO Doc 9303

3.2 Risk Assessment

Financial institutions shall implement a risk-based approach to e-KYC. Higher-risk customers or transactions must be subjected to enhanced due diligence measures, which may include additional verification steps or manual review by trained personnel.

3.3 Third-Party e-KYC Service Providers

Where financial institutions engage third-party providers to deliver e-KYC functions, they remain fully responsible for compliance with these guidelines. A formal due diligence assessment of the third-party provider must be conducted prior to engagement and reviewed annually thereafter.

4. Data Protection and Privacy

All personal data collected through e-KYC processes must be handled in accordance with the Personal Data Protection Act 2010 (PDPA). Financial institutions must

ensure:

- Explicit customer consent is obtained prior to data collection
- Data is encrypted both in transit (TLS 1.2 or above) and at rest (AES-256)
- Biometric data is stored for a maximum period of 4 years from account closure
- Regular penetration testing is conducted on e-KYC infrastructure

5. Reporting and Compliance

Financial institutions shall submit quarterly reports to the Supervision Department detailing:

Report Item	Frequency	Submission Deadline
e-KYC onboarding volume and success rates	Quarterly	15th of following month
Fraud and false positive rates	Quarterly	15th of following month
System downtime and incident reports	Monthly	5th of following month

6. Revision History

Version	Date	Summary of Changes
1.0	1 Jan 2024	Initial issuance
1.1	1 Apr 2024	Added requirements for third-party e-KYC service providers
1.2	1 Jul 2024	Biometric retention reduced from 5 to 4 years

and 277 of the Islamic Financial Services Act 2013.