BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Management of Customer Information and Permitted Disclosures

Applicable to:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks and international Islamic banks
4. Licensed insurers
5. Licensed takaful operators and international takaful operators
6. Prescribed development financial institutions
7. Approved issuers of designated payment instrument and designated Islamic payment instrument
8. Approved operators of a payment system
9. Approved insurance brokers and takaful brokers
10. Approved financial advisers and Islamic financial advisers
11. Approved money brokers
12. Registered operators of a payment system
13. Registered adjusters

Issued on: 31 October 2025 BNM/RH/PD 028-65

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 Financial service providers (FSPs) handle a significant amount of customer information in the course of providing financial services and products. Proper handling of customer information is essential in building public trust and confidence and in mitigating reputational damage to the FSPs. It is therefore critical for FSPs to protect customer information against theft, loss, misuse or unauthorised access, modification or disclosure by whatever means, including disclosure made in verbal or written form.

1.2 This Policy Document sets out Bank Negara Malaysia's (BNM) requirements and expectations with regard to FSPs' measures and controls in handling customer information, throughout the information lifecycle, covering collection, storage, use, transmission, sharing, disclosure and disposal of customer information in line with the laws administered by BNM such as the Financial Services Act 2013 (FSA), Islamic Financial Services Act 2013 (IFSA) and Development Financial Institutions Act 2002 (DFIA).

1.3 This Policy Document also sets out the conditions specified by BNM with regard to the disclosure of customer information in accordance with the permitted disclosures set out in Schedule 11 of the FSA and IFSA as well as the Fourth Schedule of the DFIA.

2 Applicability

2.1 Part B of this Policy Document is applicable to all FSPs as defined in paragraph 5.2, including their directors and officers.

2.2 Part C of this Policy Document is only applicable to financial institutions as defined in paragraph 5.2, including their directors and officers.

3 Legal provisions

3.1 The requirements in this Policy Document are specified pursuant to-
(a) sections 18(2), 47(1), 123(1) and 143(1) of the FSA;
(b) sections 57(1), 135(1) and 155(1) of the IFSA; and
(c) sections 41(1), 42C(1) and 116(1) of the DFIA.

3.2 The conditions set out in Part C are specified pursuant to-
(a) section 134(2) of the FSA;
(b) section 146(2) of the IFSA; and
(c) section 120(2) of the DFIA.

3.3 The guidance in this Policy Document is issued pursuant to section 266 of the FSA, section 277 of the IFSA and section 126 of the DFIA.

4 Effective date

4.1 This Policy Document comes into effect on 31 October 2025.

5 Interpretation

5.1 The terms and expressions used in this Policy Document must have the same meanings assigned to them in the FSA, IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this Policy Document-

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretive, 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;

"Board" refers to the board of directors of a FSP, including a committee of the Board where the responsibilities of the Board set out in this Policy Document have been delegated to such a committee. However, the Board remains fully accountable for any authority and responsibilities delegated to such committee;

"customer" refers to any person who uses, has used or may be intending to use[1], any financial service or product including-

(a) a representative of the customer (such as the parents of a minor and authorised representative[2]); and
(b) a person who has entered or intends to enter into an arrangement with a FSP (such as a guarantor or third party security provider) on account of or for the benefit of a customer;

"customer information" refers to any information relating to the affairs or, in particular, the account, of any particular customer of any FSP in whatever form including in the form of a record, book, register, correspondence, other document or material;

[1] 'Any person who may be intending to use' refers to a potential customer who has provided his/her information to the FSP for purposes of using the FSP's financial service or product, including a person who subsequently withdraws his/her application or whose application has been rejected by the FSP.
[2] Any person authorised by a customer to act on his/her behalf, for example, a trustee, someone with power of attorney, a legal guardian, an insurance agent authorised by a customer.

"disclosure" refers to disclosure by transmission, transfer, dissemination or by any other means, including verbally or in writing, by which customer information is made available by any person who has access to such customer information to another person;

"financial institution" refers to-
(a) a financial institution as defined under section 131 of the FSA;
(b) an Islamic financial institution as defined under section 143 of IFSA; and
(c) a prescribed institution as defined under section 3(1) of the DFIA;

"financial service provider" or **"FSP"** refers to-
(a) a licensed bank;
(b) a licensed investment bank;
(c) a licensed Islamic bank;
(d) a licensed international Islamic bank;
(e) a licensed insurer[3];
(f) a licensed takaful operator[4];
(g) a licensed international takaful operator;
(h) a prescribed institution;
(i) an approved insurance broker;
(j) an approved takaful broker;
(k) an approved financial adviser;
(l) an approved Islamic financial adviser;
(m) an approved money broker;
(n) an approved issuer of a designated payment instrument;
(o) an approved issuer of a designated Islamic payment instrument;
(p) an approved operator of a payment system;
(q) a registered operator of a payment system[5]; and
(r) a registered adjuster;

"outsourcing arrangement" refers to an arrangement in which a service provider performs an activity on behalf of a FSP on a continuing basis[6], where the activity would otherwise be undertaken by the FSP and does not include activities set out in Appendix 2 of the policy document on Outsourcing[7];

"outsourced service provider" or **"OSP**" refers to an entity, including an affiliate[8], providing services to a FSP under an outsourcing arrangement and includes all sub-contractor(s);

[3] Includes a professional reinsurer.
[4] Includes a professional retakaful operator.
[5] Refers to operator of a payment system that enters into a contract with a merchant for the purpose of accepting payment instruments for payment of goods or services, i.e. merchant acquirer.
[6] For the avoidance of doubt, an agreement which is time-bound does not preclude the activity from being considered as being performed on a continuing basis.
[7] For avoidance of doubt, e-money issuers and merchant acquirers are also required to comply with the outsourcing provisions outlined in the Policy Document on Electronic Money issued on 31 January 2025, and Policy Document on Merchant Acquiring Services issued on 15 September 2021.
[8] An affiliate refers to any corporation that controls, is controlled by, or is under common control with a FSP.

"representatives and agents" refer to any individual or firm acting on behalf of a FSP, which include insurance agents, takaful agents and bancassurance agents;

"senior management" refers to the chief executive officer and senior officers of FSPs;

"staff" refers to persons employed by a FSP, including temporary or contract staff, and officers on attachment from an entity within the group of the FSP.

6 Related policy documents and legal instruments

6.1 This Policy Document must be read together with any relevant legal instruments, policy documents and guidelines issued by BNM including any amendments or reissuance thereafter, in particular-

(a) Guidelines on Data Management and MIS Framework issued on 29 August 2011 (BNM/RH/GL 018-1);
(b) Guidelines on Data Management and MIS Framework for Development Financial Institutions issued on 5 November 2012 (BNM/RH/GL 005-15);
(c) Policy Document on Operational Risk issued on 10 May 2016 (BNM/RH/PD 028-15);
(d) Policy document on Outsourcing issued on 23 October 2019 (BNM/RH/PD 028-93);
(e) Policy Document on Risk Management in Technology (RMiT) issued on 1 June 2023 (BNM/RH/PD 028-98);
(f) Policy Document on Issuance of Operational Risk Reporting and Commencement of Operational Risk Reporting System issued on 10 April 2025 (BNM/RH/PD 028-128);
(g) Policy document on Product Transparency and Disclosure issued on 2 December 2024 (BNM/RH/PD 028-136); and
(h) Notifications on Disclosure of Customer Information for the National Fraud Portal (BNM/RH/NT 028-222).

6.2 The Personal Data Protection Act 2010 (PDPA), including any amendments made to the PDPA, in particular, the Personal Data Protection (Amendment) Act 2024 and any legal instruments, standards or codes issued under such law.

7 Policy documents or circulars superseded

7.1 This Policy Document supersedes the following:

(a) Policy document on Management of Customer Information and Permitted Disclosures issued on 3 April 2023; and
(b) BNM's Letter on Disclosure of Customer Information to Lembaga Hasil Dalam Negeri issued on 18 February 2022.

PART B POLICY REQUIREMENTS

The extent and degree to which a FSP implements these policy requirements must commensurate with the size of the FSP, the nature and complexity of its operations, the amount and sensitivity of customer information held as well as the potential impact on the FSP and its customers in the event of a customer information breach.

8 Board oversight

S 8.1 The Board must set the tone-at-the-top on the importance of safeguarding customer information and the potential consequences on the FSP in the event of a customer information breach. The Board shall also exercise its oversight function in all matters pertaining to the proper handling of customer information.

S 8.2 The Board must approve the FSP's written policies and ensure that written policies[9], procedures[10] and controls are in place to provide adequate protection over the confidentiality and security of customer information.

S 8.3 The Board must oversee the implementation and maintenance of the policies and procedures, including reviewing reports relating to the management of customer information from senior management. These reports should include risk assessments, findings, and mitigation plans. The Board must be satisfied that the policies, procedures and controls are adequate and effective in safeguarding customer information. These reports and mitigation plans must be periodically reviewed to reflect changes in the operating environment and evolving risks, ensuring continued relevance and effectiveness.

S 8.4 The Board must require written assurance from senior management annually that the controls in place to protect customer information are working effectively and the FSP's outsourced service providers fulfil their obligations in accordance with the contract provisions on safeguarding customer information.

9 Senior management

S 9.1 Senior management must be responsible and accountable for establishing and implementing procedures including effective systems and controls to safeguard customer information.

S 9.2 Senior management must also designate a person of sufficient senior ranking with the overall responsibility for the implementation and on-going maintenance of policies, procedures and controls with regard to safeguarding customer information. The responsibilities of the designated officer must include, but are not limited to-

[9] Policies refer to documented principles that express a FSP's goals and objectives and determine the formulation of strategy, plans, actions and procedures.

[10] Procedures refer to detailed steps to be followed as a consistent approach to put into action the policies approved by the Board in day-to-day operations.

(a) communicating relevant policies throughout the FSP to ensure consistent implementation of processes and procedures; and
(b) coordinating with key stakeholders within the FSP to comply with this Policy Document.

G 9.3 FSPs may consider establishing or designating an existing position such as the chief data officer, chief information officer or data protection officer to carry out the responsibilities in paragraph 9.2.

S 9.4 Senior management must also place the responsibility on the business and functional lines of the FSP in preserving the confidentiality and security of customer information.

S 9.5 Senior management must ensure that the FSP's appointed representatives and agents also have in place appropriate and adequate control measures to properly safeguard customer information.

S 9.6 Senior management must communicate a clear message to staff and the FSP's appointed representatives and agents, on the importance of preserving the confidentiality and security of customer information.

S 9.7 Senior management must also ensure that adequate training on relevant policies is provided to staff and that the appointed representatives and agents provide adequate training to their staff.

S 9.8 Senior management must ensure that an independent review is carried out at least once in every two years in accordance with paragraphs 10.53, 10.54, 10.55 and 10.56 on the effectiveness of policies, procedures and control measures in protecting customer information.

S 9.9 Senior management must notify the Board upon the detection of customer information breaches, depending on the nature of the breach and sensitivity of the customer information.

S 9.10 Senior management must also report to the Board on the findings of the investigation of customer information breaches, in accordance with paragraph 11.21.

10 Control environment

A. Risk assessment

S 10.1 FSPs must identify and address potential threats and vulnerabilities that could result in theft, loss, misuse, or unauthorised access, modification or disclosure by whatever means, of customer information.

S 10.2 FSPs must also assess the likelihood that identified threats and vulnerabilities will materialise, and the potential impact on both the FSP and its customers in the event a customer information breach occurs. This assessment, among other considerations, must include third-party service providers and outsourcing arrangements, and be supported by mitigation plans that are developed and implemented based on the threats identified.

G 10.3 Threats and vulnerabilities to customer information can be internal or external and could be due to negligence or a deliberate act of any person.

S 10.4 FSPs must ensure the risk assessment referred to under paragraph 10.2 is proportionate to the size, nature and complexity of the FSP's operations as well as the amount and sensitivity of customer information held.

G 10.5 FSPs may leverage on the existing arrangements, functions or tools that have a similar focus on managing risks to the confidentiality and security of customer information.

B. Policies and procedures

S 10.6 FSPs must establish and have in place written policies and procedures to safeguard customer information, and this must include the collection, access, storage, use, transmission, sharing, disclosure and disposal of customer information.

S 10.7 The written policies and procedures must be proportionate to the FSP's size, nature and complexity of the FSP's operations and the amount and sensitivity of customer information the FSP handles.

S 10.8 Without limiting the generality of paragraphs 10.6 and 10.7, FSPs must have clear written policies and procedures governing these areas-

(a) off-site work arrangements that allow access to customer information in the FSP's systems;
(b) handling and transporting of physical documents containing customer information outside the FSP's premises;
(c) the use of portable IT equipment and data storage devices; and
(d) customer information breach incident handling.

G 10.9 FSPs may incorporate the requirements on the proper handling of customer information in other policies, if appropriate. These may include written policies on human resource, code of conduct, information security, outsourcing and the disclosure of customer information to parties permitted under the law.

S 10.10 FSPs must ensure that the written policies and procedures are readily accessible and clearly communicated to staff by the person designated under paragraph 9.2, to ensure compliance with such policies and procedures.

S 10.11 FSPs must continually review their written policies and procedures to ensure that they remain adequate, relevant and operate effectively in response to changes in the operating environment.

C. Control measures

Information and communication technology (ICT) controls

S 10.12 FSPs must deploy preventive and detective ICT controls to-
(a) prevent theft, loss, misuse or unauthorised access, modification or disclosure of customer information; and
(b) detect errors and irregularities when they occur.

S 10.13 FSPs must regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats.

S 10.14 On occasions where FSPs' staff, representatives and agents undertake offsite work arrangements, FSPs must have in place appropriate controls for such offsite work arrangements including for the ICT equipment used that allow access into FSPs' systems and customer information.

G 10.15 The controls referred to in paragraph 10.14 may include robust authentication for remote access into FSPs' systems, encrypting data stored on the ICT equipment and ensuring data transmission is securely protected.

S 10.16 FSPs must ensure that only staff with a legitimate business need is allowed to download customer information into portable storage devices provided by the FSP.

S 10.17 FSPs must put in place the relevant controls to ensure that the customer information stored in such portable storage devices pursuant to paragraph 10.16 is adequately protected, such as password and data encryption, to prevent theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.

S 10.18 FSPs must ensure that staff are given access to call recordings on a strictly "need-to-know" basis for recorded telephone conversations with customers that contain customer information.

G 10.19 FSPs may consider disabling USB ports and CD writers on desktop and laptop computers of staff who do not have any operational need to download, transmit or store customer information.

S 10.20 FSPs must have in place mechanisms that create a strong deterrent effect against unauthorised disclosure by whatever means of customer information by staff.

G 10.21 Unauthorised disclosure may occur in many ways and forms such as staff taking photograph of documents or screens that contain customer information. The mechanisms referred to in paragraph 10.20 may include raising staff awareness on the disciplinary actions for unauthorised disclosure by whatever means, installing CCTV at relevant areas, having an open office concept, encouraging whistleblowing in this respect, or restricting personal electronic devices at high risk areas like data centres, dealing rooms, call centres, etc.

S 10.22 FSPs must restrict access to web-based communication websites and social media platforms, particularly those which are encrypted from end-to-end (e.g., WhatsApp Desktop, Facebook and Skype Messenger) on staff who handle customer information, to prevent unauthorised disclosure of customer information to external parties via internet services.

S 10.23 FSPs must also implement mechanisms for the prompt detection of-

(a) unauthorised access to customer information;
(b) unusual frequent viewing of customer information in the FSPs' systems by staff;
(c) unusual or suspicious downloading activities that involve customer information; and
(d) unauthorised disclosure of customer information to external parties.

G 10.24 The mechanisms referred to in paragraph 10.23 may include installing key-logger software, conducting regular reviews of audit trail and carrying out random periodic sample checks.

Access controls

S 10.25 FSPs must ensure that the role profile for each type of job includes a description of the access rights to customer information if relevant, for staff to perform their jobs in accordance with the access rights.

S 10.26 FSPs must identify the location of customer information residing in different systems and ensure that adequate access controls are in place at different levels (i.e. application level, database level, operating system level and network level) to prevent unauthorised access, modification or disclosure by whatever means of customer information to external parties.

S 10.27 FSPs must regularly review the access rights of staff and immediately revoke the access rights of any staff leaving the FSP or changing to a new role or position that does not require access to customer information to prevent the theft of customer information.

Physical security

S 10.28 FSPs must implement adequate physical security controls to ensure customer information stored either in paper or electronic forms are properly protected against theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.

S 10.29 FSPs must restrict access and implement robust intruder deterrents in areas where large amounts, or critical and sensitive customer information, are accessible and stored, for example, the server and filing rooms.

G 10.30 To minimise the risks of theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information, FSPs may consider implementing a clear-desk policy.

S 10.31 FSPs must provide clear policy and procedures encompassing adequate controls to be put in place for the proper handling of customer information collected off-site and in-transit. This must include ensuring that physical documents are securely stored while the customer information stored in portable devices are securely protected to prevent theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.

S 10.32 To effectively safeguard customer information throughout its lifecycle, FSPs must have proper procedures in place to identify customer information that is no longer required from the perspective of the operation or requirements of any written law. FSPs shall deploy appropriate methods to securely dispose of such customer information which includes any paper and digital records of the customer information.

G 10.33 Customer information is considered securely disposed of when it is beyond any possibility of recovery, is irreversible or cannot be reconstructed in any way.

G 10.34 To ensure secure data destruction, all devices may undergo proper sanitization using industry standard method and chain of custody controls, such as data wiping software, physical destruction or degaussing. For information stored in digital devices, a simple file deletion or reformatting of hard drives and portable storage devices may not be sufficient to completely destroy the stored information.

S 10.35 FSPs must assess the risks and benefits of engaging an outsourced service provider for the destruction of customer information which involves transporting customer information outside the FSP's premises.

S 10.36 FSPs must shred or store customer information in a manner that is inaccessible such as sealed in bags with tamper proof fasteners or stored in locked containers before it is collected by outsourced service providers for destruction.

S 10.37 FSPs must conduct random checks on the collection and destruction process carried out by outsourced service providers to ensure that customer information is properly destroyed.

D. Staff, Representatives, Agents and External Vendors' Personnel

G 10.38 Human factors are common contributory causes to theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. It is therefore important that all staff understand the importance of protecting the confidentiality and security of customer information.

S 10.39 FSPs must ensure that employment contracts contain a provision requiring all staff to sign a confidentiality undertaking that clearly specifies the obligation and requirement under the relevant written law to safeguard customer information as well as the consequences for failure to comply with such obligation and requirement.

S 10.40 Where FSPs engage with external vendors to carry out duties or services within the FSPs' premises (e.g., security guards, cleaners and maintenance officers/ engineers), FSPs must ensure that the external vendors carry out an appropriate level of vetting and monitoring on their personnel to reduce the risk of customer information theft.

S 10.41 FSPs must ensure a high degree of staff awareness at all times on the following:
(a) the need to protect the confidentiality and security of customer information;
(b) the importance of complying with relevant policies and procedures established by the FSPs; and
(c) the consequences if any staff is involved in any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information.

S 10.42 FSPs must have in place robust monitoring mechanisms to ensure that the relevant policies, procedures and controls established by the FSPs are adhered to by staff.

S 10.43 FSPs must provide relevant training and regularly remind all staff on their obligations to ensure the confidentiality of customer information is safeguarded when dealing with such information.

S 10.44 FSPs must include in their programme for new staff, specific trainings to explain the relevant policies and procedures on protecting customer information.

S 10.45 FSPs must ensure that new staff are notified on the possible actions that may be taken for non-compliance with policies and procedures.

G 10.46 Guidance provided to staff on safeguarding customer information should be concise and reader-friendly to enable understanding among staff on how to comply with the relevant policies and procedures.

S 10.47 FSPs must have in place mechanisms to gauge the effectiveness of trainings to staff on safeguarding customer information.

G 10.48 The mechanisms referred to in paragraph 10.47 may include conducting an annual awareness survey to assess the level of understanding among staff on protecting the confidentiality and security of customer information and reporting a customer information breach.

S 10.49 FSPs must conduct a thorough and timely investigation upon detecting theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information by staff and take appropriate actions against the staff concerned.

S 10.50 The actions taken pursuant to paragraph 10.49 must send a strong message to all staff and act as deterrent to prevent future recurrence of the customer information breach. Where the FSP decides not to take action against the staff in breach, the reason for not taking any action must be properly documented and approved by senior management.

S 10.51 In accordance with paragraph 9.10, FSPs must report to the Board the result of the investigation and actions taken against the staff concerned.

S 10.52 FSPs shall remain accountable for the conduct and actions of their appointed representatives and agents for any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information.

E. Independent review

S 10.53 FSPs must subject their written policies, procedures and control measures for safeguarding customer information to an independent review[11] at least once in every two years.

S 10.54 FSPs must ensure that the independent review must include an assessment of the effectiveness of senior management and their oversight as well as the adequacy and effectiveness of measures undertaken by the FSP to protect customer information from theft, loss, misuse or unauthorised access, modification or disclosure by whatever means.

S 10.55 The independent reviewer under paragraph 10.53 must communicate the written findings[12] to the senior management and the Board of the FSP.

S 10.56 Based on the written findings under paragraph 10.55, senior management must ensure that appropriate and timely actions are taken to rectify any deficiencies in the control measures.

11 Customer information breaches

A. Handling customer information breaches

S 11.1 FSPs must have in place a customer information breach handling and response plan to address any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. For the avoidance of doubt, FSPs must ensure that their customer information breach handling and response plans comprise of deliberate and non-deliberate customer information breaches.

S 11.2 The plan by FSPs under paragraph 11.1 must at a minimum, include escalation procedures and a clear line of responsibility to contain and take remedial actions relating to the customer information breach to prevent any future recurrence of the breach.

[11] Independent review is to be carried out by a function independent of the business units involved in the handling of customer information, such as internal audit. There is no expectation for FSPs to engage an external party to carry out the independent review.

[12] The written findings should include the review's scope, methodologies used, findings, evidence obtained, and any limitations of the review

S 11.3 FSPs must ensure that all staff understand the escalation procedures and that the relevant staff are trained to effectively take the appropriate remedial actions for a customer information breach to protect affected customers' interests.

S 11.4 FSPs must have in place a mechanism to identify customer information breaches including those which arise from customer complaints and the FSPs must investigate the complaints promptly and properly.

S 11.5 FSPs must take appropriate mitigating actions to contain a customer information breach immediately.

S 11.6 In the event that a customer information breach at one FSP involves customer data belonging to another FSP, the FSP in which the breach occurred must promptly notify the affected FSP to ensure that timely and appropriate remedial actions are undertaken.[13]

S 11.7 FSPs must assess the impact arising from the theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information. In ascertaining the impact of the customer information breach, FSPs must have regard to, at a minimum, the following:

(a) whether the breach involved accidental errors or intentional and malicious action;
(b) the type and sensitivity of customer information involved;
(c) the number of customers affected;
(d) to whom the customer information was exposed to; and
(e) the likelihood of the customer information being used for fraudulent or other harmful purposes.

B. Notification to BNM

S 11.8 FSPs must notify BNM[14] immediately upon becoming aware of a customer information breach where the breach -

(a) poses or is likely to pose reputational risk to the FSP or a threat to public confidence and trust;
(b) causes or is likely to cause significant harm to affected customer(s); or
(c) involves or is likely to involve a large number of customers (i.e. significant scale).

S 11.9 With respect to paragraph 11.8(a), a customer information breach poses or is likely to pose reputational risk to the FSP or a threat to public confidence and trust, where the breach involves, includes but not limited to where it fulfils any of the following circumstances[15]:

(a) disclosures to a party suspected of being involved in criminal activity;

[13] For example, FSP A has control over or processes any customer information obtained from FSP B arising from a permitted disclosure. If a customer information breach occurs at FSP A, FSP A must notify FSP B immediately to ensure FSP B is aware that its customers have been affected.

[14] In addition to notifying BNM, FSPs as data controllers shall comply with the mandatory data breach notification obligation to the Personal Data Protection Commissioner as prescribed in in Section 12B of PDPA and Circular of Personal Data Protection Commissioner No.2/2025 (Data Breach Notification), effective 1 June 2025 onwards.

[15] For the avoidance of doubt, this is a non-exhaustive list.

(b) information being made public or circulated via any medium including the social media; or
(c) a customer known to the public, e.g., a celebrity or a public figure or where the breach is likely to attract media attention.

S 11.10 With respect to paragraph 11.8(b), FSPs shall consider that a customer information breach causes or is likely to cause significant harm if there is a risk that the breach:
(a) may result in financial loss, damage to or loss of property, loss of business opportunities, damage to reputation, a negative effect on credit record or threat to safety of customer(s);
(b) may be misused for illegal purposes;
(c) could enable identification of theft or fraud; or
(d) consists of sensitive customer information[16].

S 11.11 With respect to paragraph 11.8(c), FSPs shall consider that a customer information breach involves or is likely to involve a large number of customers (i.e. significant scale) if the number of affected customers exceed one thousand (1,000).

S 11.12 In the event a customer information breach meets the criteria of significant scale under paragraph 11.11, FSPs must assess the potential impact and take appropriate actions to avoid or reduce any harm on the affected customers.

S 11.13 FSPs must ensure that the assessment of significant harm is confirmed by the designated officer of sufficient senior ranking as specified under paragraph 9.2.

S 11.14 With respect to customer information breaches that have been made public and circulated via any medium such as social media, FSPs must effectively manage the reputational risk arising from it, including ensuring immediate notification to BNM under paragraph 11.8.

S 11.15 If based on FSP's assessment a customer information breach appears to involve fraud, criminal activity or may result in identity theft, FSPs must also notify the relevant law enforcement agency, as soon as practicable.

S 11.16 With respect to paragraph 11.8, the notification to BNM must, at a minimum, include the following information:
(a) a description of the customer information breach that has occurred, including the type or nature of customer information that has been affected by the breach;
(b) the number of affected customers;
(c) consequences or harm to the affected customers due to the customer information breach;
(d) potential consequences or harm to the affected customers that may arise as a result of the customer information breach; and
(e) a description of measures that have been taken or will be taken by the FSP to address the breach.

[16] Examples of sensitive customer information include security credential to access customer's account, biometric data, medical or health related information.

S 11.17 In the event the complete information as required under paragraph 11.16 is not available to be submitted to BNM as required, under paragraph 11.8, the FSP must adhere to the following:

(a) the FSP shall proceed to immediately provide BNM with all other information that is available at the time.

(b) on the information under paragraph 11.16(b), the FSP must submit the estimated number of the affected customers based on their initial assessment of the breach; and

(c) the FSP must take timely and relevant measures to determine the final number of affected customers without undue delay with respect to paragraph 11.16(b).

Once the complete information required under paragraph 11.16 is obtained, the FSP must provide this information to BNM immediately.

C. Submission of detailed investigation report

S 11.18 FSPs must carry out an investigation to ascertain the root causes of a customer information breach and determine appropriate remedial actions to prevent future recurrence. Additionally, FSPs must ensure that the investigation must be carried out by a competent party[17], overseen by a party independent of the relevant business unit where the breach occurred.

S 11.19 FSPs must complete the investigation within three (3) months upon detecting a customer information breach having regard to the complexity of the breach and table a detailed investigation report to the Board.

S 11.20 FSPs must submit the detailed investigation report and **Appendix 1** to BNM within one (1) working day upon tabling to the Board in respect of a customer information breach that-

(a) causes or is likely to cause significant harm to the affected customer(s)[18];

(b) is of significant scale (i.e., affected customers exceeds or is likely to exceed 1,000); or

(c) involves a deliberate attempt on unauthorised disclosure of customer information.

S 11.21 With respect to paragraph 11.20, FSPs must ensure that the detailed investigation report to be submitted to BNM is signed off by the designated officer of sufficient senior ranking as specified under paragraph 9.2 and shall be submitted to-

Director
Consumer and Market Conduct Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

[17] Competent party refers to a party with the relevant expertise and experience in assessing a customer information breach.

[18] For the avoidance of doubt, the definition of significant harm as specified in paragraph 11.10 shall apply for the purpose of paragraph 11.20(a).

For non-bank approved issuers of designated payment instruments and Islamic designated payment instruments as well as approved and registered operators of a payment system, the abovementioned report must be submitted to-

Director
Payment Services Oversight Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

S 11.22 If a customer information breach at one FSP involves a customer information breach belonging to another FSP, it is the responsibility of the FSP in which the customer information breach occurred to carry out of the required actions specified under paragraphs 11.18 to 11.21.

S 11.23 FSPs must put in place a register to record all customer information breaches covering the root causes, remedial actions and lessons learnt to prevent future recurrences.

S 11.24 With respect to paragraph 11.23, FSP must retain the investigation reports of all customer information breach incidents for at least seven (7) years from the date the reports are tabled to the Board.

D. Notification to affected customers

S 11.25 Where the customer information breach meets the definition of causing, or is likely to cause, significant harm as outlined in paragraph 11.10, the FSP must notify the affected customers without undue delay after the notification is made to BNM under paragraph 11.8.

S 11.26 With respect to paragraph 11.25, FSPs shall ensure any delay of the notification to the affected customers does not cause further harm to the affected customers.

S 11.27 When notifying affected customers under paragraph 11.25, FSPs must ensure that the affected customers, at a minimum, are provided with the following information:

(a) a brief description of the customer information breach that has occurred;
(b) details of the potential consequences to the customer as a result of the breach;
(c) advice on the steps that should be taken by the customer to reduce or mitigate any potential consequences[19] resulting from the breach[20];
(d) a description of the measures taken or proposed to be taken by the FSP to remedy the breach and mitigate its potential consequences; and
(e) FSP's contact details from whom more information or assistance regarding the customer information breach can be obtained.

[19] This includes any potential harm or adverse effects to the affected customer as a result of the customer information breach.

[20] Examples include monitoring account for unusual activities, being alert to phishing emails and phone calls, changing password where customers' access credentials have been compromised, etc.

S 11.28 FSPs must ensure that notification to the affected customers is clear and written in plain language. The FSP must draw the customers' attention to the steps that they should take to protect themselves from any potential consequences in view of the customer information breach.

S 11.29 FSPs must notify the affected customers directly[21]. However, in exceptional circumstances where direct notification would entail disproportionate effort[22], the FSP may issue a public announcement and display prominent notices[23] at the FSP's branches and websites, provided such measures are sufficient.

S 11.30 For the avoidance of doubt, in the event an FSP is unable to identify the specific customer(s) who are affected by a customer information breach at the point it is required to notify the affected customer under paragraph 11.25, the FSP must first notify its customers generally through a public announcement and display prominent notice at the FSP's branches and website. Upon identifying the specific affected customer(s), the FSP must notify the customer(s) directly, as soon as it is feasible to do so.

S 11.31 FSPs must ensure that their staff are trained to handle queries from the affected customers and to provide the necessary assistance on protective measures against any potential consequences that could be caused by the breach.

12 Outsourced service provider

S 12.1 FSPs must monitor the risks that may arise from outsourced service providers (OSPs) with the functions of the handling of customer information.

S 12.2 FSPs must perform adequate and relevant due diligence assessments when selecting an OSP which has access to customer information including for processing, storing, or disposing customer information. These assessments will help FSPs understand the level of risks that may be introduced by the OSP and determine the appropriate monitoring that must be maintained.

S 12.3 FSPs must be satisfied that the OSP has in place policies, procedures and controls that are comparable to that of the FSPs, to ensure that customer information is properly safeguarded at all times.

S 12.4 In ensuring the obligation to safeguard customer information is adequately reflected in a Service Level Agreement (SLA)[24] with an OSP, at a minimum, the SLA must require the OSP to-

[21] Direct notification includes email, and application notification.
[22] Examples include notifying a large number of customers across multiple states or countries would impose an excessive logistical, administrative, or financial burden.
[23] The public announcement and prominent notices shall, at minimum, include the same information as stipulated under paragraph 11.28, with messaging targeted for the general public audience.
[24] For clarity, FSPs are expected to amend all of their existing relevant SLAs to comply with paragraph 12.4 and not upon renewal only.

(a) undertake to safeguard the customer information and prevent any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means, of the customer information;
(b) ensure the adequacy and effectiveness of its policies and procedures to protect the FSP's customer information;
(c) conduct robust vetting on its personnel who handles customer information;
(d) only allow its personnel to have access to customer information strictly for the purpose of carrying out the OSP's functions under the SLA;
(e) ensure that its personnel understands and undertakes to comply with the prohibition on disclosure by whatever means of customer information to any person for any purpose other than that which is specified in the SLA, permitted under the written law or approved by BNM, as the case may be (including after the end of the contract term);
(f) investigate any customer information breach to determine when and how the breach occurred;
(g) report any customer information breach to the FSP within an agreed timeframe;
(h) destroy in accordance with paragraph 10.32 or return all customer information to the FSP upon the expiry or termination of the SLA; and
(i) allow the FSP to audit or inspect how customer information is safeguarded.

G 12.5 FSPs may provide clear expectations to the OSP on the control measures required in respect of processing, storage, transmission, disposal or destruction of the FSPs' customer information.

S 12.6 FSPs must require the OSP to sign a binding non-disclosure undertaking with regard to the handling of customer information.

S 12.7 FSPs must ensure that the OSP conducts training to its personnel, at regular intervals, on relevant policies and procedures relating to the proper handling of customer information as well as reviews the adequacy and effectiveness of the training programme.

G 12.8 FSPs may consider providing training to the OSPs' personnel to promote awareness of the importance of safeguarding the FSPs' customer information and to ensure compliance with the contractual requirements.

S 12.9 FSPs must conduct a review of the OSP at least once in every two years to confirm that the OSP fulfils its obligations in accordance with the contract provisions in safeguarding the FSPs' customer information.

S 12.10 FSPs must take reasonable steps to maintain accurate and complete records and trail of all customer information that have been shared or given to the OSPs.

PART C SPECIFIC REQUIREMENTS ON PERMITTED DISCLOSURE

13 Conditions in relation to permitted disclosure

S 13.1 A financial institution, its directors and officers must comply with the conditions specified in the table below in relation to permitted disclosures of any customer information as set out under Schedule 11 of the FSA and IFSA as well as the Fourth Schedule of the DFIA.

G 13.2 For the avoidance of doubt, items 5, 6, and 7 in the table below are not applicable to prescribed institutions[25].

Purposes for or circumstances in which customer documents or information may be disclosed	Persons to whom documents or information may be disclosed	Conditions
1. Compliance with an order or request made by an enforcement agency in Malaysia under any written law for the purposes of an investigation or prosecution of an offence under any written law.	An investigating officer authorised under the written law to investigate or any officer authorised to carry out prosecution or any court.	(a) The request must be specific in relation to- i. name and identification number of the customer (to the extent known); ii. account number and type of account with the financial institution or reference information of specific document required (e.g., cheque number); iii. provision of the relevant law under which the offence is believed to have been committed; and iv. name, identity and contact information of the investigating officer to whom the customer information is to be disclosed; (b) the request must be made in writing using the application forms in

[25] This refers to development financial institutions prescribed under section 2(1) of the DFIA which currently are-
(a) Bank Pembangunan Malaysia Berhad;
(b) Bank Perusahaan Kecil & Sederhana Malaysia Berhad (SME Bank);
(c) Export-Import Bank of Malaysia (EXIM Bank);
(d) Bank Kerjasama Rakyat Malaysia Berhad;
(e) Bank Simpanan Nasional; and
(f) Bank Pertanian Malaysia Berhad (Agrobank).

		Appendix II, III and IV, as applicable;[26] (c) in the case of an order or request made by- i. Polis Diraja Malaysia (PDRM), the order or request must be signed by an officer of a rank higher than the investigating officer who must be at least an Inspector; ii. Jabatan Kastam Diraja Malaysia, the order or request must be signed by the head of division, branch, unit or station conducting the investigation; or iii. the other law enforcement agencies, the order or request must be signed by an officer of senior ranking who is in the list of the authorised signatories of the respective law enforcement agency; (d) in the case of an order or request made by PDRM via the eFSA portal[27]- i. the order or request must be made by the authorised investigating officer of PDRM attaching the following: • the digital order issued by PDRM under section 51(1) of the Criminal Procedure Code (Act 593); and • the eFSA form (with controlled serial numbers on three key references, namely, eFSA application reference, Commercial Crime Intelligence System

[26] The templates in Appendix II, III and IV are the standard forms to be used for the purposes of requesting for a customer's information or document under the FSA, IFSA and DFIA, as the case may be.

[27] The eFSA portal is a secured digital platform developed and administered by the Commercial Crime Investigation Department (CCID) of PDRM that allows online submission of a request for customer information to financial institutions for purposes of an investigation or prosecution of an offence under any written law. The eFSA portal also allows the uploading of customer information by financial institutions to PDRM. For any submission by PDRM via eFSA, condition (d) will replace conditions (b) and (c).

		(CCIS) reference number and identification number of the investigating officer); ii. the financial institution must conduct adequate validation or verification to ensure that it is accessing a genuine order or request from PDRM via the eFSA portal. In validating or verifying the request from PDRM submitted via eFSA portal, the financial institution must- • verify the identity and authority of the investigating officer requesting the information; and • verify the consistency of the controlled serial numbers on key references in the digital order and eFSA form; iii. the financial institution shall only upload the customer information requested by the authorised investigating officer pursuant to the digital order issued by PDRM under section 51(1) of the Criminal Procedure Code (Act 593) into the eFSA portal after performing adequate validation or verification to ensure that it is accessing the actual eFSA portal and not a phishing site; and iv. if in doubt, the financial institution must contact PDRM to confirm the validity of the order or request, the eFSA portal as well as the attachments or accompanying information. A financial institution must promptly report any irregularities observed to the PDRM for assessment and rectification, where relevant;

		(e) the financial institution must make reasonable enquiries to confirm that a request or order is properly authorised; (f) the financial institution must verify the identity and authority of the investigating officer to whom customer information is disclosed, including sighting identification and authorisation documents (e.g., authority card); and (g) in the event the law enforcement agency requests to take possession of, make copies of, or remove from the financial institution's premises, any customer information, financial institutions must ensure that the law enforcement agency and its officers are empowered by the respective written law to do so.
2. Documents or information is required by the Inland Revenue Board of Malaysia (IRBM) under section 81 of the Income Tax Act 1967 (ITA) for the purpose of- a) facilitating exchange of information pursuant to taxation arrangements or agreements having effect under sections 132, 132A or 132B of the ITA; or b) making an application to court for a garnishee order in accordance with section 106A of the ITA.	Any officer of the IRBM or any persons authorized by IRBM to receive the documents or information on its behalf.	The following are conditions applicable to the disclosure of customer information pursuant to sections 132 and 132A of the ITA: (a) the financial institution has received a notice in writing issued by the IRBM pursuant to section 81 of ITA that clearly identifies the customer under examination or investigation; (b) the financial institution has received a statement from IRBM confirming that the customer from whom the information is required has failed to comply with a notice issued pursuant to section 81 of ITA and the Income Tax (Exchange for Information) Rules 2011 [P.U.(A) 219/2011] within the time specified in the notice; and (c) the financial institution must notify the customer of the information that has been furnished to IRBM. The financial institution is not required to

		do so if IRBM has not made a prior request to the customer for the information. IRBM will state the specific circumstances in which this situation arises in the written notice. This includes circumstances where the request is of an urgent nature or in the case where prior notification to the customer is likely to undermine the actions of the foreign applicant authority. The following are the conditions applicable to the disclosure of customer information pursuant to section 106A of the ITA: (a) the financial institution has received a notice in writing issued by IRBM pursuant to section 81 of the ITA (Notice) requiring for the disclosure of the customer information for the purpose of section 106A of the ITA. The Notice must, at minimum, set out the name and identification number of the customer; (b) the financial institution must ensure that the Notice is signed by either one of the authorised signatories of IRBM, i.e. the Director of Legal Department or Director of Civil and Prosecution Division; (c) the financial institution must ensure that IRBM has attached to the Notice a copy of the judgement obtained against the taxpayer in a civil proceeding instituted by IRBM in accordance with section 106 of the ITA; and (d) if the financial institution has any doubt on the authenticity of the Notice or any of its attachments, the financial institution must contact IRBM to verify the authenticity of the Notice or any of its attachments.
3. Performance of functions of the	Any person engaged by the financial institution	(a) The financial institution must comply with all relevant requirements applicable to

financial institution which are outsourced.	to perform the outsourced function	outsourcing arrangements as may be specified by BNM; and (b) the person having access to the customer information must enter into a binding non-disclosure agreement with the financial institution.
4. Disclosure to a consultant or adjuster engaged by the financial institution.	Consultant or adjuster engaged by the financial institution.	(a) A consultant refers to any person that provides professional advice, independent assessment or services on a particular field of expertise (e.g., corporate strategy, treasury, operations management, IT, market survey) to financial institutions, on a temporary basis for a fee. A consultant may also be engaged when financial institutions lack the necessary capacity or resources for a specific project (e.g., to implement new business processes); (b) where the consultant or adjuster has been engaged by the head office / financial holding company, the financial institution must be a party to the agreement between the head office / financial holding company and the consultant concerned; (c) the disclosure of customer information must be strictly on a need-to-know basis; (d) access to customer information by the consultant or adjuster (both local and foreign) is restricted to the financial institution's premises in Malaysia[28]; and

[28] This condition will not apply where the information disclosed is in the form of a summary or collection of information set out in such manner as does not enable information relating to any particular customer of the financial institution to be ascertained from it, or at the time of disclosure the information has already been made lawfully available to the public from any source other than the financial institution.

		(e) the consultant or adjuster having access to the customer information must enter into a binding non-disclosure agreement with the financial institution.
5. Performance of any supervisory functions, exercise any of supervisory powers or discharge any of supervisory duties by a relevant authority outside Malaysia which exercises functions corresponding to those of BNM under the FSA or IFSA.	Any officer of the relevant authority authorised to receive the documents or information.	(a) The relevant authority outside Malaysia must be the foreign supervisory authority responsible for the group-wide supervision of the financial group to which the financial institution belongs; (b) a request for customer information must be made by the authority outside Malaysia in writing to the financial institution stating the purpose for which the information is required; (c) no information relating to deposit accounts must be disclosed to the authority outside Malaysia; (d) BNM must be notified of any provision of customer information to the authority outside Malaysia. Such notification must be submitted to Pengarah, Jabatan Penyeliaan Konglomerat Kewangan, Pengarah, Jabatan Penyeliaan Perbankan, or Pengarah, Jabatan Pemantauan Pembayaran as applicable; and (e) the financial institution must obtain an undertaking from the officers of the relevant authority authorised to receive the customer information that the customer information must be used for the sole purpose of performing a supervisory function and such information will not be revealed to any other party.

6. Conduct of centralised functions, which include internal audit, risk management, finance or information technology or any other centralised function within the financial group.	The head office or holding company of a financial institution whether in or outside Malaysia or any other person[29], designated by the head office or holding company to perform such functions.	(a) Centralised functions refer to functions established at a regional office or the head office for the purposes of group oversight and compliance with regulatory requirements. They exclude any ad hoc assignments or one-off activity to be carried out by the regional or head office[30]; (b) the disclosure of customer information must be strictly on a need-to-know basis; (c) the head office or holding company must be a regulated financial institution or a regulated institution which is subject to equivalent obligations under any law or regulation (in or outside Malaysia) which protects confidentiality of customer information; and (d) the financial institution must comply with all relevant regulatory requirements and conditions applicable to centralised functions as may be specified by BNM.
7. Due diligence exercise approved by the board of directors of the financial institution in connection with- (a) merger and acquisition; (b) capital raising exercise; or (c) sale of assets or whole or part of business	Any person participating or otherwise involved in the due diligence exercise approved by the board of the financial institution.	(a) The disclosure must only be made to the named individuals responsible for the due diligence exercise and must be time-bound; (b) the person having access to the customer information must enter into a binding non-disclosure agreement with the financial institution; and (c) customer information must only be disclosed after the financial institution has obtained the approval of BNM or the Minister of

[29] Which may include an external party.
[30] For the avoidance of doubt, a centralised function differs from an outsourced function in which the latter is performed by a service provider, an affiliate or shared service centre, on behalf of the financial institution.

		Finance, as the case may be, in respect of: (i) the capital raising exercise or sale of assets or business; or (ii) a merger and acquisition.
8. Documents or information which is permitted in writing by the customer, the executor or administrator of the customer, or in the case of a customer who is incapacitated, any other legal personal representative.	Any person permitted by the customer or, as the case may be, the executor, administrator or legal personal representative.	Effective from 1 January 2024, a financial institution seeking a consent[31] from the customer, executor, administrator or legal personal representative of the customer must comply with the following conditions[32]: a) **specific** - The financial institution must ensure that the terms seeking a customer's consent are clear, concise, and written in plain language. Further, the relevant terms must be specific in relation to the following: (i) The person to whom the disclosure will be made[33]; (ii) the purpose of such disclosure; and (iii) the information that will be disclosed; b) **voluntary**[34] - The financial institution must not, as a condition of providing a financial product/service, compel or coerce a customer to give consent for the disclosure of his/her information to third parties beyond what is necessary for the provision

[31] These conditions are applicable to financial institutions seeking customers' consent for the disclosure of their information to third parties from 1 January 2024 onwards. These conditions do not apply to consent obtained from customers prior to the effective date.

[32] These conditions are relevant only if the financial institution discloses customers' information to third parties based on the customers' consent. These conditions do not apply to other scenarios whereby the disclosure of customer information is already permitted under the FSA/IFSA/DFIA, such as the disclosure of customers' credit information to a credit reporting agency registered under the Credit Reporting Agencies Act 2010.

[33] It would be sufficient for the financial institution to indicate the categories of third parties to whom the customer information will be disclosed subject to controls in place to protect the information. For example, disclosure to business partners for the promotion of financial products/services. It is unacceptable to use descriptions of third parties which are too broad or vague, such as disclosure to any third parties as the financial institution deems fit.

[34] Consent is not considered as "voluntary" if customers are unable to refuse to provide their consent or feel compelled to give their consent for the disclosure of their information to third parties beyond what is necessary for the provision of the financial product/service or the performance of the contract. For example, this includes the disclosure of customer information to third parties for marketing and promotional purposes where consent is secured using a pre-ticked option box which requires customers to opt-out of such arrangement.

		of the financial product/service or the performance of the contract with the customer. The financial institution is prohibited from obtaining a customer's consent by asking the customer to indicate consent to a statement or term that combines agreement to the disclosure of his/her information with other matters in a single statement of consent[35]; c) **explicit and deliberate**[36] - A customer must explicitly opt in or deliberately agree[37] to the disclosure of his/her customer information by the financial institution to a third party. Hence, silence or inaction on the part of the customer does not constitute an explicit and deliberate consent by the customer. The financial institution is prohibited from obtaining a customer's consent using pre-ticked[38] consent statements; and d) **revocable upon request**, subject to the requirements of applicable laws and for the provision of the financial product/service to the customer[39] - A customer must be allowed to withdraw or revoke his/her consent for the disclosure of his/her information at any time, unless such

[35] Where consent is sought as a condition for the provision of a financial product/service, the consent does not meet the requirement of being "voluntary" since customers are unable to refuse giving their consent. For example, this includes combining the request for consent to disclose customers' information to a third party for marketing purposes within a clause to inform customers that their information are collected for the provision of the product/service. In other words, the request for customers' consent must be a standalone clause/term.

[36] For consent to be valid, customers must have taken a deliberate action to provide consent to the disclosure of their information. A customer's failure to opt out of a consent statement or term is not considered a valid consent as it does not involve an explicit and deliberate action by the customer.

[37] For example, signing a consent form, ticking an opt-in box on paper or electronically, or clicking an opt-in button online.

[38] A pre-ticked consent box in a product/service application form does not meet the requirement of being an "explicit and deliberate" consent by a customer as there is no way to definitively establish that the customer consented to the pre-ticked box and the applicable statement/term.

[39] This condition only affects the disclosure of customer information for purposes that are based on customers' consent. The financial institution must allow customers to withdraw or revoke their consent without terminating the product/service unless the disclosure of customer information is necessary for the financial institution to comply with any legal requirements or contractual obligations. In other words, the withdrawal of consent for the disclosure of customer information would not affect performance of the contract by the financial institution.

		disclosure is necessary for the financial institution to comply with any legal or contractual requirements. Further, the customer must be informed of his/her rights to withdraw or revoke the consent and how to effect such withdrawal or revocation of consent. The process for withdrawing consent must be as straightforward as it was to obtain the consent, for example via online platforms. The financial institution must cease the disclosure of customer information based on the customer's consent as soon as practicable after the withdrawal of the consent. A reasonable time frame would be not more than 7 calendar days from the day the financial institution receives the withdrawal of consent notice. The financial institution shall also allow existing customers to withdraw their consents given before the effective date, unless the disclosure of customer information affects the ability of the financial institution to comply with any legal or contractual requirements. The financial institution shall maintain records of any customer consent it has relied upon when making such disclosure in a manner that is accessible, wherein the financial institution must be able to produce such evidence upon request by the customer or relevant authorities including BNM.

S 13.3 Financial institutions are required to put in place adequate control measures over the disclosure of customer information to any parties which are permitted under the FSA, IFSA or DFIA, which at a minimum shall include-

(a) the processes to be undertaken by the officers responsible to verify the authenticity of the orders or requests;

(b) documentation requirements; and

(c) authority levels for approving disclosure of customer information which must be at an appropriate senior level.

S 13.4 Financial institutions intending to apply for BNM's approval for the disclosure of customer information under section 134(1)(b) of the FSA, section 146(1)(b) of the IFSA or section 120(1)(b) of the DFIA must complete and submit the application form in **Appendix V** to BNM.

Appendix I: Template for reporting customer information breach

INFORMATION ON CUSTOMER INFORMATION BREACH	
A.	**Details of the customer information breach**
1.	Date of reporting to BNM
2.	Name of party (ies) who has committed the breach *(Please provide any HR record to show that the party concerned is a staff; or evidence to show that the party concerned is a staff of an OSP)*
3.	Type of customer information where the party in item 2 was given access
4.	Name and details of the recipient of the customer information (i.e. occupation and relationship to the party (ies) in item 2)
5.	Details of information disclosed (*Please provide a copy of all relevant documents, including evidence of disclosure made*)
6	Name of customer(s) whose information has been disclosed
7.	Date of incident
8.	Time of incident
9.	Place of disclosure
10.	Details of incident (including the chronology of events)
B.	**Details of breach handling**
1.	Party who investigates the customer information breach and prepares the findings
2.	How the customer information breach was detected? *(e.g., via complaint, internal audit,etc.)*
3.	Root cause(s) of the customer information breach
4.	Remedial actions taken or that will be taken (to provide timelines and the relevant supporting documents)
5.	Details on the escalation to the board (to attach the board meeting minutes)

Officer-in-charge,
- Signature -
…….
Name:
Contact number:

Note: FSPs must use the Excel template provided

Appendix II: Application form for PDRM

PERMOHONAN MAKLUMAT / DOKUMEN INSTITUSI KEWANGAN
OLEH PEGAWAI-PEGAWAI PENYIASAT POLIS DIRAJA MALAYSIA (PDRM)

☐ Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013
☐ Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013
☐ Seksyen 120 (2) Akta Institusi Kewangan Pembangunan 2002

A.	**Butiran Pegawai Penyiasat**	
1.	**Nama Penuh:**	
2.	**Jawatan:**	
3.	**No. Kad Kuasa:**	
4.	**Alamat Pejabat & No. Faks:**	
5.	**No. Telefon Pejabat / Bimbit:**	
6.	**Alamat e-mel:**	
B.	**Butiran maklumat berhubung penyiasatan**	
1.	**Seksyen Kesalahan:**	
2.	**No. Laporan Polis:**	
C.	**Butiran maklumat yang dikehendaki berhubung dengan siasatan dan pendakwaan (Sila tandakan "TB" (Tidak Berkaitan) pada ruang yang tidak berkenaan)**	
1.	**Nama Pemegang Akaun (Jika ada): (Individu/Persatuan/Syarikat/Perniagaan)**	
2.	**No. Kad Pengenalan (Baru/Lama)/Pasport/ No. Pendaftaran Syarikat/Perniagaan (Jika ada):**	
3.	**Nama Institusi Kewangan:**	
4.	**Maklumat Akaun / Dokumen:**	
	a) No. Akaun / No. Cek / No. Siri	
	b) Jenis Akaun / Produk Kewangan	
	c) Sijil Seksyen 90A Akta Keterangan 1950 untuk Dokumen yang dikeluarkan Komputer	☐ YA ☐ TIDAK
5.	**Maklumat CCTV**	
	a) Lokasi	
	b) Tarikh / Masa	
6.	**Tandatangan & Cop Pegawai Penyiasat**	
D.	**Pengesahan Pegawai Polis yang lebih kanan daripada Pegawai Penyiasat (Inspektor dan ke atas)**	
	Nama Pegawai & No. Kad Kuasa	
	Tandatangan / Tarikh	
	Cop Rasmi	

Appendix III: Application form for Jabatan Kastam Diraja Malaysia

PERMOHONAN MAKLUMAT / DOKUMEN INSTITUSI KEWANGAN OLEH JABATAN KASTAM DIRAJA MALAYSIA

☐ Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013
☐ Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013
☐ Seksyen 120 (2) Akta Institusi Kewangan Pembangunan 2002

A.	**Butiran Pegawai yang menjalankan siasatan**	
1.	**Nama Penuh:**	
2.	**Jawatan:**	
3.	**No. Kad Kuasa:**	
4.	**Alamat Pejabat & No. Faks:**	
5.	**No. Telefon Pejabat/ Bimbit:**	
6.	**Alamat e-mel:**	
B.	**Butiran maklumat berhubung penyiasatan**	
1.	**Seksyen Kesalahan:**	
2.	**No. Rujukan Fail Siasatan:**	
C.	**Butiran maklumat yang dikehendaki berhubung dengan siasatan dan pendakwaan (Sila tandakan "TB" (Tidak Berkaitan) pada ruang yang tidak berkenaan)**	
1.	**Nama Pemegang Akaun (Jika ada): (Individu / Persatuan / Syarikat / Perniagaan)**	
2.	**No. Kad Pengenalan (Baru/Lama)/ Pasport/ No. Pendaftaran Syarikat/ Perniagaan (Jika ada):**	
3.	**Nama Institusi Kewangan:**	
4.	**Maklumat Akaun / Dokumen:**	
	a) No. Akaun / No. Cek / No. Siri	
	b) Jenis Akaun / Produk Kewangan	
	c) Sijil Seksyen 90A Akta Keterangan 1950 untuk Dokumen yang dikeluarkan Komputer	☐ YA ☐ TIDAK
5.	**Maklumat CCTV**	
	a) Lokasi	
	b) Tarikh/Masa	
6.	**Tandatangan & Cop Pegawai yang menjalankan siasatan**	
D.	**Tandatangan Pegawai Kanan Kastam yang mengetuai Bahagian/Cawangan/Unit/Stesen**	
	Nama	
	Jawatan	
	Bahagian/ Cawangan/ Unit/ Stesen	
	Tandatangan / Tarikh	
	Cop Rasmi	

Appendix IV: Application form for law enforcement agencies other than PDRM and Jabatan Kastam Diraja Malaysia

PERMOHONAN MAKLUMAT / DOKUMEN INSTITUSI KEWANGAN OLEH AGENSI PENGUATKUASA UNDANG-UNDANG		
☐ Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013 ☐ Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013 ☐ Seksyen 120 (2) Akta Institusi Kewangan Pembangunan 2002		
A.	**Nama Agensi Penguatkuasa Undang-Undang:**	
B.	**Butiran Pegawai Penyiasat**	
1.	**Nama Penuh:**	
2.	**Jawatan:**	
3.	**No. Kad Kuasa:**	
4.	**Alamat Pejabat & No. Faks:**	
5.	**No. Telefon Pejabat/ Bimbit:**	
6.	**Alamat e-mel:**	
C.	**Butiran maklumat berhubung penyiasatan**	
1.	**Seksyen Kesalahan:**	
2.	**No. Rujukan Fail Siasatan:**	
D.	**Butiran maklumat yang dikehendaki berhubung dengan siasatan dan pendakwaan (Sila tandakan "TB" (Tidak Berkaitan) pada ruang yang tidak berkenaan)**	
1.	**Nama Pemegang Akaun (Jika ada): (Individu / Persatuan / Syarikat / Perniagaan)**	
2.	**No. Kad Pengenalan (Baru/Lama)/ Pasport/ No. Pendaftaran Syarikat/ Perniagaan (Jika ada):**	
3.	**Nama Institusi Kewangan:**	
4.	**Maklumat Akaun / Dokumen:**	
	a) No. Akaun / No. Cek / No. Siri	
	b) Jenis Akaun / Produk Kewangan	
	c) Sijil Seksyen 90A Akta Keterangan 1950 untuk Dokumen yang dikeluarkan Komputer	☐ YA ☐ TIDAK
5.	**Maklumat CCTV**	
	a) Lokasi	
	b) Tarikh / Masa	
E.	**Tandatangan Pegawai Berkuasa yang dibenarkan menjalankan siasatan[1]**	
	Nama / Jawatan	
	Tandatangan / Tarikh	
	Cop Rasmi	

[1]Seperti di dalam senarai pegawai berkuasa yang dibenarkan menjalankan siasatan daripada agensi penguatkuasa undang-undang berkenaan.

Appendix V: Application for Disclosure of Customer Information

Name of Financial Institution:

Application for approval pursuant to: *(please tick)*

☐	Section 134(1)(b) of the Financial Services Act 2013
☐	Section 146(1)(b) of the Islamic Financial Services Act 2013
☐	Section 120(1)(b) of the Development Financial Institutions Act 2002

Details of application:

Disclosure by	
Disclosure to	
Purpose of disclosure	
Period of disclosure	
Types of customer information to be disclosed	
Manner of Disclosure	
Safeguards in place to preserve the confidentiality of customer information	

Officer-in-charge,

- Signature -
…….
Name:
Contact number:
E-mail address:
Date:

Note: FSPs must use the Excel template provided