



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 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 payment system
13. Registered adjusters

Issued on: 17 October 2017

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 policy documents and legal instruments.....	4
7	Policy documents or circulars superseded	4
PART B	POLICY REQUIREMENTS.....	5
8	Board oversight	5
9	Senior management	5
10	Control environment	6
11	Customer information breaches.....	12
12	Outsourced service provider	14
PART C	SPECIFIC REQUIREMENTS ON PERMITTED DISCLOSURE	16
13	Conditions in relation to permitted disclosure	16
Appendix I:	Template for reporting customer information breach	23
Appendix II:	Application form for PDRM	24
Appendix III:	Application form for Jabatan Kastam Diraja Malaysia	25
Appendix IV:	Application form for law enforcement agencies other than PDRM and Jabatan Kastam Diraja Malaysia.....	26
Appendix V:	Application for Disclosure of Customer Information	27

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 (the Bank) 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 the Bank 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 the Bank with regard to 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 17 October 2017.
- 4.2 The Bank is committed to ensure its policies remain relevant and continue to meet the intended objectives and outcome. Accordingly, the Bank will review this policy document within five years from the date of issuance and where necessary, amend or replace this policy document.

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 use¹, any financial service or product including-

- (a) a representative of the customer (such as the parents of a minor and authorised representative²); and
- (b) a person who has entered or intend to enter into arrangement with FSPs (such as a guarantor or third party security provider) on account of or for the benefit of a customer;

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 withdraw 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.

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

“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 the 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;
- (f) a licensed takaful operator;
- (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; and
- (r) a registered adjuster;

“outsourcing arrangement” is an arrangement in which an outsourced service provider performs an activity on behalf of a FSP on a continuing basis, where the activity is normally or could be undertaken by the FSP³;

“outsourced service provider” or **“OSP”** refers to entity, including an affiliate⁴, providing services to a FSP under an outsourcing arrangement and includes all sub-contractor(s);

³ For the avoidance of doubt, system or application leveraging, data center hosting, data center operations, data storage, cloud computing services and back-up location(s) are considered as outsourcing arrangements.

⁴ 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; and

“**staff**” refers to persons employed by a FSP, including temporary or contract staff, and officers on attachment from an affiliate⁵.

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 the Bank, in particular-

- (a) Data Management and MIS Framework;
- (b) Data Management and MIS Framework for Development Financial Institutions;
- (c) Managing Cyber Risks;
- (d) Managing Cyber Risks on Remote Desktop Protocol;
- (e) Management of IT Environment;
- (f) Operational Risk;
- (g) Operational Risk Reporting Requirement - Operational Risk Integrated Online Network;
- (h) Outsourcing of Banking Operations;
- (i) Outsourcing of Islamic Banking Operations;
- (j) Outsourcing for Insurers;
- (k) Outsourcing for Takaful Operators; and
- (l) Outsourcing for Development Financial Institutions; and
- (m) Product Transparency and Disclosure.

6.2 The Personal Data Protection Act 2010 and any legal instruments, standards or codes issued under such law are also relevant.

7 Policy documents or circulars superseded

7.1 This policy document supersedes the policy documents listed below:

- (a) Disclosure of Customer Documents or Information issued on 2 July 2013 (FSA and IFSA); and
- (b) Disclosure of Customer Documents or Information issued on 15 July 2016 (DFIA).

⁵ An affiliate refers to any corporation that controls, is controlled by, or is under common control, with a FSP.

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 policies⁶ and ensure procedures 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. The board must be satisfied that the policies, procedures and controls are adequate and effective in safeguarding customer information.
- S** 8.4 The board must require 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 held accountable for establishing and implementing procedures⁷ 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 must include, but are not limited to-
 - (a) communicating relevant policies throughout the FSP to ensure consistent implementation of processes and procedures; and

⁶ Policies refer to documented principles that express a firm's goals and objectives and determine the formulation of strategy, plans, actions and procedures.

⁷ 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.

(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 or chief information 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 of 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 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 11.8.

10 Control environment

A. Risk assessment

- S** 10.1 FSPs must identify potential threats and vulnerabilities that could result in theft, loss, misuse, or unauthorised access, modification or disclosure by whatever means.
- S** 10.2 FSPs must also assess the likelihood that such threat and vulnerability will materialise and the potential impact it will have on the FSP and its customers in the event a customer information breach occurs.

- G** 10.3 Threats and vulnerabilities to customer information can be internal or external and could be due to negligence or deliberate act of any person.
- S** 10.4 The risk assessment by FSPs must be 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 existing arrangements, functions or tools that have a similar focus on managing risk 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, which covers collection, storage, use, transmission, sharing, disclosure and disposal of customer information.
- S** 10.7 The policies and procedures must be appropriate 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 paragraph 10.6 and 10.7, FSPs must have clear 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 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 proper handling of customer information in other policies, if appropriate. For instance, human resource policy, code of conduct, information security policy, outsourcing policy and policy dealing with the disclosure of customer information to parties permitted under the law.
- S** 10.10 The FSPs must ensure that the 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 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 prevent theft, loss, misuse or unauthorised access, modification or disclosure of customer information and to 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 for 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 Customer information stored in such portable storage devices pursuant to paragraph 10.16 must be adequately protected by relevant controls 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 is given access to call recordings strictly on a "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) for 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 the job.
- 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 a 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 employ robust intruder deterrents to areas where large amounts of customer information is 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 include ensuring that physical documents are securely stored while customer information stored in portable devices is 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 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 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 fastener 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 contract contains a provision requiring all staff to sign a confidentiality undertaking that clearly specifies the obligation and requirement of any 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 officer/engineer), 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 FSP; and
 - (c) the consequences if 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 to ensure that the relevant policies, procedures and controls established by the FSPs are being adhered to by staff.
- S** 10.43 FSPs must provide relevant training and regularly remind all staff on their obligations to properly handle customer information.
- S** 10.44 FSPs must include in their programme for new staff a specific training to explain the relevant policies and procedures on protecting customer information.
- S** 10.45 New staff must also be alerted by the FSPs 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 of customer information.
- G** 10.48 The mechanisms referred to in paragraph 10.47 may include conducting annual awareness survey to assess the level of understanding among staff on protecting the confidentiality and security of customer information and reporting customer information breaches.
- 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. 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 policies, procedures and control measures for safeguarding customer information to an independent review⁸ at least once in every two years.
- S** 10.54 The independent review must include an assessment of the effectiveness of senior management and its 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 its findings to senior management and the board.
- S** 10.56 Based on the findings, senior management must ensure that appropriate and timely actions are taken to rectify any deficiencies in the control measures.

11 Customer information breaches

- S** 11.1 FSPs must have in place a customer information breach handling and response plan in the event of theft, loss, misuse or unauthorised access, modification or disclosure by whatever means of customer information.
- 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 the customer information breach and take remedial actions.
- S** 11.3 FSPs must ensure that staff understands the escalation procedures and relevant staff are trained to take the appropriate remedial action to a customer information breach effectively 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 investigate the complaints promptly and properly.

⁸ 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.

- S** 11.5 FSPs must take appropriate mitigating actions to contain a customer information breach immediately.
- S** 11.6 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.
- S** 11.7 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. The investigation must be carried out by a competent party⁹, overseen by a party independent of the business unit where the breach occurred.
- S** 11.8 FSPs must complete the investigation within three months upon detecting a customer information breach, having regard to the complexity of the breach. FSPs must submit a detailed investigation report and **Appendix I** to the Bank within one working day upon tabling to the board. The report, signed off by a senior officer, must be submitted to:
- Pengarah
Jabatan Konsumer dan Amalan Pasaran
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
- S** 11.9 Where the customer information breach is likely to pose reputational risk to FSPs or a threat to public confidence and trust, FSPs must notify the Bank immediately upon discovery of the breach.
- G** 11.10 The customer information breach referred to in paragraph 11.9 includes cases where-
- (a) the customer information has been disclosed to a party suspected of being involved in criminal activity;
 - (b) it involves or likely to involve a large number of customers due to system failures or weaknesses;
 - (c) the customer information has been made public or circulated via any medium including the social media; or
 - (d) it involves a customer known to the public, e.g. a celebrity or a public figure or the breach is likely to attract media attention.

⁹ Competent party refers to a party with the relevant expertise and experience in assessing a customer information breach.

- S** 11.11 If the breach appears to involve fraud, criminal activity or may result in identity theft, FSPs must also notify the relevant law enforcement agency.
- S** 11.12 In the event the customer information breach affects a large number of customers, FSPs must assess the potential impact and take appropriate actions to avoid or reduce any harm on the affected customers.
- G** 11.13 The actions referred to in paragraph 11.12 may include the following:
- (a) making a public announcement to notify the customers promptly to regain customers' confidence;
 - (b) providing contact details for customers to obtain further information or raise any concern with regard to the breach; or
 - (c) providing advice to affected customers on protective measures against potential harm that could be caused by the breach.
- S** 11.14 FSPs must have in place a register to record all customer information breaches covering the root causes, remedial actions and lessons learnt to prevent future recurrences.

12 Outsourced service provider

- S** 12.1 FSPs must monitor the risks that may arise from OSPs with the functions of 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 the Service Level Agreement (SLA)¹⁰ with an OSP, at a minimum, the SLA must require the OSP to:
- (a) undertake to safeguard the customer information and prevent any theft, loss, misuse or unauthorised access, modification or disclosure by whatever means;
 - (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 access to customer information strictly for the purpose of carrying out their functions;

¹⁰ For clarity, FSPs are expected to amend all of their existing relevant SLAs to comply with paragraph 12.4 and not upon renewal only.

- (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 the Bank, 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 staff, 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' staff 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 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 below in relation to permitted disclosures of any customer information as set out under Schedule 11 of the FSA and IFSA as well as 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 institutions¹¹.

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: <ol style="list-style-type: none"> 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; iv. name, identity and contact information of the investigating officer to whom the customer information is to be disclosed;

¹¹ This refers to developed 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).

		<p>(b) The request must be made in writing using the application forms in Appendix II, III and IV, as applicable;¹²</p> <p>(c) In the case of an order or request made by:</p> <ul style="list-style-type: none"> i. the Police, 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; 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; <p>(d) The financial institution must make reasonable enquiries to confirm that a request or order is properly authorised;</p> <p>(e) The financial institution must verify the identity and authority of the investigating officer to whom customer information is disclosed, including citing identification and authorisation documents (e.g. authority card); and</p> <p>(f) In the event that the law enforcement agency requests to take possession of, make copies of, or remove from the financial institution's premises, any</p>
--	--	--

¹² The forms in Appendix II, III and IV will be the standard forms to be used for purposes of requesting for customer's information or document under the Financial Services Act 2013, Islamic Financial Services Act 2013 and Development Financial Institutions Act 2002, as the case may be.

		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 purposes of facilitating exchange of information pursuant to taxation arrangements or agreements having effect under section 132 or 132A of the Income Tax Act 1967.	Any officer of the Inland Revenue Board of Malaysia authorised to receive the documents or information.	<p>(a) The financial institution has received a notice in writing issued by IRBM pursuant to section 81 of ITA that clearly identifies the customer under examination or investigation;</p> <p>(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</p> <p>(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.</p>
3. Performance of functions of the financial institution which are outsourced.	Any person engaged by the financial institution to perform the outsourced function	<p>(a) The financial institution must comply with all relevant requirements applicable to outsourcing arrangements as may be specified by the Bank; and</p> <p>(b) The person having access to the</p>

		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.	<p>(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);</p> <p>(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;</p> <p>(c) The disclosure of customer information must be strictly on a need-to-know basis;</p> <p>(d) Access to customer information by the consultant or adjuster (both local and foreign) is restricted to the financial institution's premises in Malaysia¹³; and</p> <p>(e) The consultant or adjuster having access to the customer information</p>

¹³ 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.

		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 the Bank under the FSA or IFSA.	Any officer of the relevant authority authorised to receive the documents or information.	<p>(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;</p> <p>(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;</p> <p>(c) No information relating to deposit accounts must be disclosed to the authority outside Malaysia;</p> <p>(d) The Bank 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 or Pengarah, Jabatan Penyeliaan Perbankan, as applicable; and</p> <p>(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.</p>
6. Conduct of centralised functions, which include internal audit, risk management, finance or information	The head office or holding company of a financial institution whether in or outside	(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

<p>technology or any other centralised function within the financial group.</p>	<p>Malaysia or any other person¹⁴, designated by the head office or holding company to perform such functions.</p>	<p>requirements. They exclude any ad hoc assignments or one-off activity to be carried out by the regional or head office¹⁵;</p> <p>(b) The disclosure of customer information must be strictly on a need-to-know basis;</p> <p>(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</p> <p>(d) The financial institution must comply with all relevant regulatory requirements and conditions applicable to centralised functions as may be specified by the Bank.</p>
<p>7. Due diligence exercise approved by the board of directors of the financial institution in connection with-</p> <p>(a) merger and acquisition;</p> <p>(b) capital raising exercise; or</p> <p>(c) sale of assets or whole or part of business</p>	<p>Any person participating or otherwise involved in the due diligence exercise approved by the board of the financial institution.</p>	<p>(a) The disclosure must only be made to the named individuals responsible for the due diligence exercise and must be time-bound;</p> <p>(b) The person having access to the customer information must enter into a binding non-disclosure agreement with the financial institution; and</p> <p>(c) Customer information must only be disclosed after the financial institution has obtained the approval of the Bank or the Minister of Finance, as the case may be, in respect of:</p> <p>(i) the capital raising exercise or</p>

¹⁴ Which may include an external party.

¹⁵ 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 center, on behalf of the financial institution.

		sale of assets or business; or (ii) a merger and acquisition.
--	--	--

- S** 13.3 Financial institutions are required to put in place adequate controls over the disclosure of customer information to any parties which are permitted under the FSA, IFSA or DFIA. The control measures must, at a minimum, include-
- (a) the processes to be undertaken by responsible officers 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 the Bank's approval for 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 the Bank.

Appendix I: Template for reporting customer information breach

INFORMATION ON CUSTOMER INFORMATION BREACH	
A. Details of breach	
1.	Date of reporting to BNM
2.	Name of party (ies) who has committed the breach <i>(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)</i>
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 in item 2)
5.	Types / details of information disclosed <i>(Please provide a copy of all relevant documents, including evidence of disclosure made)</i>
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 event)
B. Details of breach handling	
1.	Party who investigates the customer information breach and prepares the findings
2.	How was the breach detected? <i>E.g. via complaint, internal audit, etc.</i>
3.	Root cause(s) of the customer information breach
4.	Remedial actions taken or will be taken (to provide timelines and relevant documents)
5.	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)	
<input type="checkbox"/>	Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013
<input type="checkbox"/>	Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013
<input type="checkbox"/>	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
	<input type="checkbox"/> YA <input type="checkbox"/> 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	
<input type="checkbox"/>	Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013
<input type="checkbox"/>	Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013
<input type="checkbox"/>	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
	<input type="checkbox"/> YA <input type="checkbox"/> 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		
<input type="checkbox"/> Seksyen 134 (2) Akta Perkhidmatan Kewangan 2013 <input type="checkbox"/> Seksyen 146 (2) Akta Perkhidmatan Kewangan Islam 2013 <input type="checkbox"/> 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	<input type="checkbox"/> YA <input type="checkbox"/> TIDAK
5.	Maklumat CCTV	
	a) Lokasi	
	b) Tarikh / Masa	
E. Tandatangan Pegawai Berkuasa yang dibenarkan menjalankan siasatan¹		
	Nama / Jawatan	
	Tandatangan / Tarikh	
	Cop Rasmi	

¹Seperti 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)*

- | | |
|--------------------------|--|
| <input type="checkbox"/> | Section 134(1)(b) of the Financial Services Act 2013 |
| <input type="checkbox"/> | Section 146(1)(b) of the Islamic Financial Services Act 2013 |
| <input type="checkbox"/> | 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	
Safeguards in place to preserve the confidentiality of customer information	

Officer-in-charge,

- Signature -

.....

Name :

Contact number :

E-mail address :

Date :