NOTICE TO BANKS AND ISLAMIC BANKS

NOTICE NO. TRS/N-1/2020/1

EARLY DETECTION OF CYBER INTRUSION AND INCIDENT REPORTING

---

1. INTRODUCTION

1.1 This Notice is issued pursuant to section 66 of the Banking Order, 2006 and section 66 of the Islamic Banking Order, 2008 and applies to all banks and Islamic banks in Brunei Darussalam. This Notice is also expected to be adhered to by Perbadanan Tabung Amanah Islam Brunei established under the Perbadanan Tabung Amanah Islam Brunei Act (Chapter 163) to the same extent as banks.

1.2 In light of the recent rise in cybersecurity incidents happening around the world, it is becoming more likely that financial institutions are being targeted by cybercriminals. Their techniques are also becoming more sophisticated such as by exploiting vulnerabilities, using ransomware and spear phishing. While traditional cybersecurity tools are appropriate in preventing malwares with known signatures, such strategies are gradually losing their effectiveness against more sophisticated cyber-attacks that leverage on zero-day and exploits. Many studies have repeatedly shown that most organisations were unaware of a breach in their systems and networks long after it has taken place. In many cases, external parties rather than the organisation itself discovered the breach. Such delays in detecting cyber intrusions have compromised the interests of the organisations and their customers, and potentially disrupt financial stability. The Autoriti Monetari Brunei Darussalam (AMBD) therefore places great emphasis on the requirements for banks to continuously enhance their detection of cyber intrusion and to report any major IT incidents to AMBD.

1.3 This Notice shall take immediate effect.

2. DEFINITIONS

2.1 For the purpose of this Notice, and unless otherwise expressly stated, all words and terms in this Notice shall have the same meaning as used in the Banking Order, 2006 (for banks) or Islamic Banking Order, 2008 (for Islamic banks).

2.2 "Authorised communication channel" refers to email, mobile phone, letter or other channel that has been agreed between a bank and AMBD.

2.3 "Bank" includes both banks and Islamic banks.

2.4 "Critical system" refers to any system that supports the provision of bank services, where failure of the system can significantly impair the bank's provision of services to its customers or stakeholders, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements.

2.5 "Cyber intrusion" is the act of accessing a network, system, server, end-point or IT device without authorisation or consent.

2.6 "End-point" refers to any computer or laptop used for a bank's work purposes and to store information related to the bank, its stakeholders and customers.

2.7 "IT incident" means any disruption, malfunction, error, cyber intrusions or cybersecurity issues on a bank's system, server, network or end-point that has an impact on its operations and service delivery. An IT incident may be categorised according to Schedule 1.

2.8 "Major IT incident" refers to an IT incident which has a severe and widespread impact on a bank's operations and service delivery, or has a material impact to a bank.

2.9 "Material impact" refers to an IT incident which results in severe damage or consequence to a bank. This includes IT incidents relating to financial, reputational, data confidentiality, operational, legal and/or compliance aspects.

2.10 "Near-miss IT incident" means an IT incident that has no or partial material impact to a bank but where, given a period of time, may have a material impact to the bank, and any other IT incidents which can be categorised as a minor or moderate type of IT incident.

2.11 "Network" refers to the computer networks on a bank's work premise that are used in conducting its work activities.

2.12 "Server" refers to servers that are managed by a bank that hosts its system(s).

2.13 "System" means any hardware, software, network or other IT component which is part of an IT infrastructure.

2.14 "Third-party service provider" refers to a third party providing services in relation to networks, servers, software and systems. This does not include non-IT related services including, but not limited to, physical transfer of funds, security guards, maintenance of hardware and facilities, cleaning services and subscription to online news.

3. EARLY DETECTION OF CYBER INTRUSION

3.1 A bank shall ensure that there are systematic and consistent procedures in place for risk identification, assessment, responses and monitoring in relation to IT incidents including cyber intrusion on the bank's IT systems and environments. Risk assessments are to be performed regularly and on an ad-hoc basis to determine the likelihood and severity of any impacts due to cyber intrusion.

3.2 A bank shall monitor incoming and outgoing network traffic on their network to detect and/or block suspicious external network events. For example, a bank should put in place devices, software and/or other appropriate capabilities to detect anomalous traffic from external entity into the bank's systems or from the bank's systems to an unknown external entity.

3.3 A bank must monitor internal network communications closely to detect and/or block unauthorised network communications amongst servers, systems and end-point devices. For example, a bank should put in place devices, software tools, sensors and/or other appropriate capabilities to detect anomalous traffic across systems within the internal networks.

3.4 A bank shall put in place mechanisms to detect and/or block behavioural anomalies on the bank's systems, servers and devices. Examples of such activities include unusual user access pattern, unauthorised system configuration changes, and/or abnormal memory access and system processes. As affected devices often attempt to establish connections to the command and control servers through internet connections, the bank must proactively monitor and block these indicators.

3.5 Upon confirmation of a successful cyber intrusion, the bank shall perform a thorough investigation to determine the extent of the cyber intrusion and damage sustained as well as to identify the vulnerabilities being exploited by the attacker. While the investigation is ongoing, the bank shall take immediate actions to contain the situation in order to prevent further damage and commence recovery efforts to restore operations based on their response plan.

4. INCIDENT REPORTING

4.1 Upon confirmation of a successful cyber intrusion or from the confirmation that an incident is categorised as a major IT incident (collectively referred to in this paragraph 4 as "Incident"), the bank shall notify Technology Risk Supervision of AMBD no later than **two (2) hours** after confirmation of the Incident either via email, telephone call or other authorised communication channel. In any event, the bank shall not make any public announcement regarding the Incident prior to such notification to AMBD.

4.2 Where an Incident has been confirmed, the bank shall provide timely updates to AMBD on the progress of their incident handling, business continuity and service restoration at least once every day via telephone call or other authorised communication channel until the Incident has been resolved.

4.3 A bank shall submit a root-cause and impact analysis report(s) ("IT Incident Report") to the Technology Risk Supervision of AMBD through email **within 5 working days**, or such longer period as AMBD may allow, from the confirmation of the Incident. The bank is to submit the IT Incident Report in such form and manner as may be determined by the AMBD.

4.4 A bank shall record and compile all near-miss IT incidents that are confirmed. Subsequently, the bank must submit the recorded and compiled details to AMBD within 5 working days after the **end of each month** in such form and manner as may be determined by AMBD.

5. RECOVERY TIME OBJECTIVE

5.1 It is the expectation of the public and other stakeholders for any bank to deliver service without delays or interruption which may occur due to intermittent or inoperable critical systems. In this regard, a bank shall put in place a framework and process in identifying and assessing its own critical systems.

5.2 A bank shall make all reasonable efforts in maintaining high availability of its critical systems. Each unplanned downtime (D1) of the bank's critical systems will have a validity of 12 months period (V1) from the date of occurrence. Where a subsequent unplanned downtime occurs (D2) during V1, the cumulative downtime period of both D1 and D2 shall not exceed 240 minutes. At the expiry of V1, and subject to there being no further unplanned downtime occurring, the downtime period for D2 remains until V2 has expired. Without limiting the generality of this paragraph 5.2, the following illustration may be considered:

A bank experienced unplanned downtime on their critical system, System A on 1st January 2018 for 180 minutes. Then on 31st May 2018, that bank experienced another unplanned downtime on their System A for 30 minutes. Assuming that there is no other unplanned downtime between 1st January and 31st May 2018, the total system A downtime for the 12 months' period from 1st January to 31st May is 210 minutes. Commencing 1st January 2019, the total system A downtime would be 30 minutes rather than 210 minutes.

However, if the bank experienced unplanned downtime on 30th April 2019, the total unplanned downtime for system A would be calculated as 30 minutes + the unplanned downtime on 30th April 2019 until the unplanned downtime recorded on 31st May 2018 expires on 30th May 2019.

6. GAP ANALYSIS

6.1 A bank shall regularly perform risk assessments, gap analysis and testing at least once a year against relevant technology-related notices and guidelines issued by AMBD, international IT standards and industry best practices to ensure its controls remain appropriate and adequate, and that its response and business continuity plans remain effective. The bank shall also put in place effective measures, processes and procedures to promptly address any gaps that are found.

6.2 A bank shall ensure that it has in place policies and procedures on incident handling (including incident categorization), business continuity and service restoration. The bank shall periodically review at least once a year and, where necessary, update its policies and procedures on incident handling, business continuity and service restoration by considering new and changing IT incident trends.

MANAGING DIRECTOR

AUTORITI MONETARI BRUNEI DARUSSALAM

Issue Date: 18 August 2020

SCHEDULE 1

IT INCIDENT CATEGORISATION

This schedule provides guidance for banks in determining categories of IT incidents based on the impact severity of IT incidents. This list is **non-exhaustive** and is without prejudice to the generality of the definitions of "Major IT Incident" and "Near-miss IT Incident".

Minor	a) Known or reported phishing emails using the bank's identity or information directed to customers and stakeholders, but no malware or fraud took place. b) Downtime or error in network, server, software and system that cause minimal or no impact to the bank's daily operations but if not managed or rectified in time, can escalate to moderate or major incident. c) Lease line failure (to primary data center or other key IT services) but backup line was activated almost immediately (less than 10 minutes). d) Incidents caused by a third-party service provider that have minimal or no impact to the bank's daily operation and service delivery. e) Local end-user issue such as software errors or hardware failure that can hinder operation or service delivery. f) Network intrusion attempt that are detected but successfully blocked at the firewall, IDS/IPS or other security devices.
Moderate	a) Downtime or error in network, server, software and system that have partial impact on the bank's daily operation. b) There is a failure in leased line (to primary data center or other key IT services); however, backup was activated within more than 10 minutes but less than 1 hour.

	c) IT disruption caused by a third-party service provider that restricts or delays services or causes intermittent service of the bank's daily operation. d) Malware attack whether successful or blocked, on less than 5 users with no known data breach. e) Attempted spear phishing attack that is directed to at least two employees, but no successful fraud took place. f) Persistent and targeted network intrusion attempts that are detected but successfully blocked at the firewall, IDS/IPS or other security devices.
Major	a) Downtime causes the bank's daily operation to be completely inoperable for more than 1 hour. b) Downtime causes the bank's daily operation to be reduced (less than 20% of the system is operating). c) Downtime or error in network, server, software and system that have a financial impact of at least B$500,000 per incident on the bank. d) Any IT issues that causes official local or international media coverage (i.e. news, newspaper), penalties, fine and/or lawsuit on the bank. e) Data breach (including data loss, data leak and stolen data) and ransomware that affect the bank's classified data and/or compromise personal data of customers, employees and stakeholders. f) Malware outbreak that spreads through the bank's network or directly on the bank's critical system or any other devices in use for the purpose of the bank's daily operations; excluding personal devices that are used for personal purposes. g) Website defacement or unauthorised modification to the bank's general website, social media page and/or smartphone apps.

	h) Successful cyber intrusion or unauthorised access into the bank's network, server or end-point. i) Insider breach (including but not limited to sabotage or social engineering) by any person (including disgruntled employees) that affect the bank's operation and classified data. j) Successful cyber-crimes or fraud activities on the bank conducted over the bank's technology channels. k) Lease line (to primary data center or other key IT services) failure with back up line not activated according to the bank's recovery time objective or as per agreed in any relevant service level agreement. l) IT disruption caused by a third-party service provider that has a material impact to the bank's daily operations. m) IT performance issues that affect important bulk processing jobs, where the bank is unable to run the job on the same business day. n) Recurring IT incidents of a similar nature which has occurred more than 5 times within a 12 month period. The recurring incidents should be assessed to determine the root cause. If the root cause resulted from weaknesses that can lead to major IT incidents, the findings should be reported as a major IT incident.