Amendment No. 1

Effective date of Amendment No. 1: 1 January 2024

NOTICE FOR BANKS AND ISLAMIC BANKS
NOTICE NO. TRS/N-1/2020/1

NOTICE ON 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. The Brunei Darussalam Central Bank (BDCB) may, at its discretion, take supervisory action against any banks or Islamic banks if it fails to comply with any of the provisions under this Notice.

[Amendment No. 1 dated 23 November 2023]

1.2. In light of recent rise in cybersecurity incidents happening in Brunei Darussalam and globally, it is becoming more likely that Banks 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. BDCB therefore places great emphasis on the requirements for Banks to continuously enhance their detection of cyber intrusion and to report major IT incidents to BDCB.

[Amendment No. 1 dated 23 November 2023]

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 Banks and BDCB during working hours, non-working hours and holiday period.

[Amendment No. 1 dated 23 November 2023]

2.3. "Banks" includes both conventional banks and Islamic banks.

2.4. "Critical system" refers to any system that supports the provision of Banks' services, where failure of the system can significantly impair the Banks' 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. "Downtime" refers to disruption on IT system, infrastructure or service, which affect availability of IT systems, or service delivery to consumers.

[Amendment No. 1 dated 23 November 2023]

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

2.8. "IT incident' means disruption, malfunction, error, cyber intrusions or cybersecurity issues on the Banks' 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.

2.9. "Major IT incident" refers to an IT incident which has a severe and widespread impact on the Banks' operations and service delivery, or has a material impact to the Banks.

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

2.11. "National incident reporting requirement" refers to any requirements to provide information on IT or cybersecurity incidents to a government agency or statutory body, other than BDCB, pursuant to requirements under a specific national legislation.

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

2.13. "Network" refers to the computer networks on Banks' work premise that are used in conducting its work activities.

2.14. "Peak period" refers to the time period when customers require the bank's services to be accessible or when there is an anticipated increase in the use of the bank's digital financial services, such as during pay day, bonus period, and festive season.

[Amendment No. 1 dated 23 November 2023]

2.15. "Planned downtime" refers to downtime scheduled by the Banks with proper planning and preparation, in order to perform maintenance, upgrade, change, repair, or testing on their critical system.

[Amendment No. 1 dated 23 November 2023]

2.16. "Potential cyber intrusion" refers to a situation where a cyber intrusion is suspected to have infiltrated the Banks critical system and network, such as when an indicator of compromise was observed by the Banks personnel or reported by a user.

[Amendment No. 1 dated 23 November 2023]

2.17. "Server" refers to servers that are managed by Banks that hosts its respective system(s).

2.18. "Suspected Incident" means a potential cyber intrusion or an unscheduled downtime on Banks' critical system, which may or may not be a major IT incident.

[Amendment No. 1 dated 23 November 2023]

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

2.20. "Systemic risk" refers to a risk event or impact that has nation-wide impact, or affects the whole financial services industry.

[Amendment No. 1 dated 23 November 2023]

2.21. "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.

2.22. "Unplanned downtime" refers to downtime that is not planned or scheduled in advance by a Bank, stemming from factors including, but not limited to, IT failure, successful cyber intrusion and emergency maintenance.

[Amendment No. 1 dated 23 November 2023]

3. EARLY DETECTION OF CYBER INTRUSION

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

[Amendment No. 1 dated 23 November 2023]

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

[Amendment No. 1 dated 23 November 2023]

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

[Amendment No. 1 dated 23 November 2023]

3.5. Upon confirmation of a successful cyber intrusion, Banks 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 Banks 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. Banks shall notify Technology Risk of BDCB no later than **one (1) hour** after the discovery of a Suspected Incident either via email, telephone call or other authorised communication channel.

[Amendment No. 1 dated 23 November 2023]

4.2. Banks shall assess the Suspected Incident and notify Technology Risk of BDCB no later than **two (2) hours** after first discovery of the Suspected Incident either via email, telephone call or other authorised communication channel whether:

4.2.1. the incident is a successful cyber intrusion or otherwise; and

4.2.2. the incident is a major IT incident or otherwise.

[Amendment No. 1 dated 23 November 2023]

4.3. Banks shall not make any public announcement regarding a Suspected Incident prior to notifying BDCB of its assessment under paragraph 4.2.

[Amendment No. 1 dated 23 November 2023]

4.4. Where a cyber intrusion or major IT incident has been confirmed under paragraph 4.2, Banks shall provide timely updates to BDCB on the progress of their incident response, including activation of business continuity plan, activation of disaster recovery plan and external stakeholder involvement at least twice every calendar day via telephone call or other authorised communication channel until the cyber intrusion or major IT incident has been resolved.

[Amendment No. 1 dated 23 November 2023]

4.5. Banks shall submit a root-cause and impact analysis report(s) ("IT Incident Report") to the Technology Risk of BDCB through email **within 5 working days**, or such longer period as BDCB may allow, from the notification to BDCB under paragraph 4.2. Banks are to submit the IT Incident Report in such form and manner as may be determined by BDCB.

[Amendment No. 1 dated 23 November 2023]

4.6. Without prejudice to any national incident reporting requirements, the Banks shall provide a copy of the national incident reporting form to BDCB when submitting the national incident reporting form to the required party.

[Amendment No. 1 dated 23 November 2023]

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

[Amendment No. 1 dated 23 November 2023]

5. RECOVERY TIME OBJECTIVE

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

[Amendment No. 1 dated 23 November 2023]

5.2. Banks shall notify Technology Risk of BDCB through e-mail at the latest five (5) working days before any planned downtime, such as performing scheduled maintenance and system migration activities. Banks shall not schedule or perform the planned downtime during peak periods. Following this notification, the Banks shall make a public announcement of the reasons and duration of the planned downtime.

[Amendment No. 1 dated 23 November 2023]

5.3. Banks shall make all reasonable efforts in maintaining high availability of its critical systems whereby the unplanned downtime (except caused by systemic risks) of each critical system shall not exceed 240 minutes (regardless of whether these were accumulated from multiple incidents or as a result of 1 single incident) within a rolling period of 12 months. Without limiting the generality of this paragraph 5.3, the following illustration may be considered:

Banks experienced unplanned downtime on their critical system, System A on 1st January 2023 for 180 minutes. Then on 31st May 2023, the Banks experienced another unplanned downtime on their System A for 30 minutes. Assuming that there is no other unplanned downtime between 1st January 2023 and 1st January 2024, the total downtime for System A from 1st January 2023 to 31st May 2023 period is 210 minutes. Commencing 1st January 2024, the total downtime of System A would be 30 minutes rather than 210 minutes, since the first unplanned downtime of 180 minutes has reached 12 months' period. However, if the Banks experienced unplanned downtime on 30th April 2023, the total unplanned downtime for System A on 1st January 2024 would be calculated as 30 minutes + the unplanned downtime on 30th April 2023. The unplanned downtime of 30 minutes recorded on 31st May 2023 shall expire on 30th May 2024.

[Amendment No. 1 dated 23 November 2023]

6. GAP ANALYSIS

6.1 Banks shall regularly perform risk assessments, gap analysis and testing against relevant technology-related Notices and Guidelines issued by BDCB, 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 Banks shall also put in place effective measures, processes and procedures to promptly address any gaps that are found.

[Amendment No. 1 dated 23 November 2023]

6.2 Banks shall ensure that it has in place policies and procedures on incident handling (including incident categorisation), business continuity and service restoration. The Banks 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
BRUNEI DARUSSALAM CENTRAL BANK

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 Banks' 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 Banks' 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 Banks' 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 Banks' 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 Banks' 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) Unplanned downtime in any critical system that causes the Bank's daily operation and service delivery to be completely inoperable for more than 30 minutes. b) Suspected Incident that cannot be verified as an Incident or false positive for more than 2 hours from the discovery of the Suspected Incident. c) Downtime causes the Banks daily operation to be completely inoperable or reduced (less than 20% of the system is operating) for more than 30 minutes. d) Downtime or error in network, server, software and system that have a financial impact of at least B$500,000 per incident on the Banks. e) Any IT issues that causes official local or international media coverage (i.e. news, newspaper), penalties, fine and/or lawsuit on the Banks. f) Data breach (including data loss, data leak and stolen data) and ransomware that affect the Banks' classified data or personal data of customers, employees and/or stakeholders. g) Malware outbreak that spreads through the Banks network or directly on the Banks critical system or any other devices used for in carrying out Banks daily operations. h) Website defacement or unauthorised modification to Banks' general website, social media page and/or smartphone apps that are visible to public. i) Successful cyber intrusion into Banks' network, server or endpoint that cannot be contained or eradicated for more than 30 minutes. j) Unauthorised access or account compromised in the Banks' IT systems including but not limited to operating system, application, and e-mail. k) Insider breach (including but not limited to sabotage or social engineering) by any person (including disgruntled employees) that affect the Banks' operation (see c) and classified data (see f). l) Successful cyber-crimes or fraud activities on the Banks conducted in the Banks IT system or over the Banks technology channels. m) Lease line failure with back up line not activated according to the Banks recovery time objective, or as per agreed in any relevant service level agreement. n) IT disruption caused by a third-party service provider that has a material impact to the Banks daily operations (see c).

	o) IT performance issues that affect important bulk processing jobs, where the Banks are unable to run the job on the same business day, affecting business operation (see c) and/or financial impact (see d) to the Banks. p) Any IT-related incident that is required to be reported by any national law and legislation.

[Amendment No. 1 dated 23 November 2023]