
# GUIDELINES TO MONEY CHANGER AND MONEY REMITTANCE BUSINESSES, AND PAWNBROKERS

GUIDELINE NO. TRS/G-5/2024/1

GUIDELINES ON TECHNOLOGY RISK MANAGEMENT

## 1. INTRODUCTION

1.1 Innovation and technological developments have transformed the way businesses and operations are being conducted. Financial institutions continuously adopt new technology to improve their businesses and to provide more advanced products and services to keep pace with their customers' expectation for smart and innovative financial services.

1.2 With businesses moving into digital space, a number of technological issues including cybersecurity incidents are also increasing. Money changer and remittance businesses, and pawnbrokers (hereafter, referred as "MCRBP") are not excluded from such risks. As such, MCRBP need to ensure they have adequate controls to manage these risks.

1.3 This Guideline is issued pursuant to section 32 of the Brunei Darussalam Central Bank (BDCB) Order, 2010 and aims to provide basic guidance to MCRBP in managing technology and cybersecurity risk based on best industry practices.

1.4 This Guideline is not exhaustive and subject to revision from time to time as deemed necessary by the Authority.

1.5 This Guideline should be read with the following:

i. Notice on Early Detection of Cyber Intrusion and Incident Reporting (Notice No. FTU/N-1/2017/1);
ii. Notice on Market Conduct (Notice No. FCI/N2/2021/1);
iii. Guidelines on IT Third Party Risk Management (Guidelines No. TRS/G-3/2022/2); and
iv. Guidelines on Minimum Standards for a Remittance System (Guidelines No. SM/G-1/2020/1).

1.6 This Guideline shall take effect on 1st November 2024 and shall supersede the Standard Technology Risk Management Guidelines (Guideline No. TRS/G-1/2019/1) which is hereby repealed.

## 2. DEFINITIONS

2.1 In this Guideline, the following terms shall have the following meanings, except where the context otherwise requires:

2.1.1 "Browser extension/plugin/add-on" refers to external software components that work in tandem with the web browser to allow additional functions;

2.1.2 "Browser tracking" refers to a method used by web browsers to track the users through cookies, website beacons, system configuration and login credentials;

2.1.3 "CERT" or "Computer Emergency Response Team" is a team of cybersecurity experts that assist or consult organisations in responding to cybersecurity incidents. In Brunei, our local CERT is BruCERT;

2.1.4 "Computer" refers to desktop, laptop or other devices used for the MCRBP's work purposes and to store information related to the business, stakeholders and customers;

2.1.5 "Cookies" are small data files that are required to be stored on a user's computer when visiting a web site to store information of the user's activity on the website;

2.1.6 "Critical data" refers to data that are identified as assets to the MCRBP, in which any loss or leak of data will lead to a severe impact to the MCRBP's competitive advantage, operations and reputation;

2.1.7 "Firewall" is a device or program that controls the flow of network traffic between networks or hosts that employ differing security postures;

2.1.8 "HTTPS" or "hypertext transfer protocol secure" is the secure version of HTTP and is the protocol used to browse websites or transfer data in the Internet;

2.1.9 "IT asset" refers to software, hardware, data and other components that makes up the IT environment (e.g. network, system and computer) of a MCRBP;

2.1.10 "IT asset register" is a database or spreadsheet containing a list and details of IT assets which include, but is not limited to, asset type, serial number, manufacturer name, supplier name, current location and purchase date;

2.1.11 "IT incident" refers to system, network, end-user or cybersecurity issues that disrupt or could potentially disrupt the MCRBP's business operations or data;

2.1.12 "IT officer" refers to personnel that manages, administers and maintains IT systems and infrastructure of the MCRBP;

2.1.13 "Material impact" refers to an IT incident which results in severe damage or consequences to an MCRBP. This includes IT incidents relating to financial, reputational, operational, legal and/or compliance aspects;

2.1.14 "Mobile devices" refers to devices that are portable enough to be brought into or taken out of an MCRBP's premise by personnel. This includes, but is not limited to, laptops, tablets and smartphones that are supplied by the MCRBP or owned by the personnel;

2.1.15 "Money changer and remittance businesses" means any person licensed to carry on any money-changing business or remittance business under the Money-Changing and Remittance Businesses Act, Cap. 174;

2.1.16 "Network" refers to the IT networks on an MCRBP's work premise that are used in conducting MCRBP business activities;

2.1.17 "One-time password" or "OTP" refers to a password sent to user through SMS, e-mail or token to authenticate user for a single session or transaction.

2.1.18 "Online services" refer to services offered by MCRBP on the Internet via web application or online portal such as online remittance service;

2.1.19 "Pawnbroker" means any person licensed to carry on the business of a pawnbroker under the Pawnbrokers Order, 2002;

2.1.20 "Phishing" is the attempt to acquire sensitive information such as usernames, passwords, and credit card details usually by impersonating a trustworthy entity through electronic communication;

2.1.21 "Server" refers to server machines that are managed by the MCRBP or third party (e.g. cloud service) to host MCRBP's system(s);

2.1.22 "SSL" or "Secure Socket Layer" refers to encryption protocols used for HTTPS;

2.1.23 "System" refers to the IT system that is used to run an MCRBP's business operations that usually consist of applications, databases, servers and network infrastructure;

2.1.24 "Third-party cookies" refers to cookies that do not belong to a website that a user visited but are still sent to the user;

2.1.25 "TLS" or "Transport Layer Security" refers end-to-end encryption protocols used for communication between web applications over the Internet.

2.1.26 "Two-factor authentication" refers to having an additional method of authentication such as software tokens or one time passwords in addition to username and password authentication;

2.1.27 "Web browser" is a software program that allows a user to locate, access, and display web pages such as Google Chrome and Windows Edge (Internet Explorer); and

2.1.28 "Wi-Fi Protected Access 2 (WPA2)" is a method of securing your network using WPA2 encryption protocol.

## 3. IT GOVERNANCE

### 3.1 Organisational Structure

3.1.1 The MCRBP should appoint at least one personnel as an IT officer that is qualified to manage IT and cybersecurity controls in the MCRBP. The IT officer may hold other roles within the MCRBP such as a compliance officer, provided that these roles do not hinder one another.

3.1.2 The MCRBP should mandate all personnel to report any IT and cybersecurity issues, and any technical requests to the IT officer.

3.1.3 The IT officer should report to its management any IT and cybersecurity related matters in the MCRBP.

## 3.2 Policy and Procedure

3.2.1 The MCRBP should include protection of data and cybersecurity practices in their workplace into its policies.

3.2.2 The MCRBP should develop policies and procedures for the management of technology in their business which includes, but is not limited to, the following areas:

a) Proper usage of IT assets including workstation, removable media and back up;
b) Safeguarding IT assets including personnel responsible to protect against unauthorised access, theft and physical damage;
c) Maintenance of IT assets including destruction and return of IT assets;
d) Management of IT assets includes controlling software installation;
e) Protection, handling and backup of information and data;
f) Handling of IT operations;
g) Issue, complaints and incident handling;
h) User access and password management including separate network connection for personnel and customers; and
i) Vendor selection, agreement and management.

3.2.3 The management should define acceptable communication channels and procedures such as the use of WhatsApp, e-mail and office phone for personnel to formally engage with stakeholders and customers.

3.2.4 The policies and procedures of the MCRBP should be reviewed on a frequent basis (i.e. yearly or every two years) and it should be communicated and made available to all personnel in the MCRBP.

3.2.5 The management of an MCRBP should impose consequences for personnel that violate the policies and procedures of the MCRBP. This also applies to employees that are no longer working with MCRBP.

3.2.6 All system and IT related documentation including administrator guides and user manuals should be kept and stored safely by the MCRBP. It is expected for the MCRBP to review and update the administrator guides and user manuals whenever there is a change in system or every year.

## 3.3 Third Party Management

3.3.1 In the event the MCRBP wishes to designate system development, maintenance, and IT operations to a third party, the MCRBP should establish risk-based third party management framework based on Paragraph 5.1 of Guidelines No. TRS/G-3/2022/2.

3.3.2 A written agreement and non-disclosure agreement should be present in all IT arrangements with third party according to Paragraph 4.8 of Guidelines No. TRS/G-3/2022/2 to ensure third parties perform their work according to their scope of work, and to protect sensitive data and information belonging to the MCRBP.

3.3.3 In the event of contract termination with the third-party vendor, either on expiry or ended prematurely, the MCRBP should have the contractual power and means to ensure that the service provider returns, removes and/or destroys information shared by the MCRBP as stated in Paragraph 4.15 of Guidelines No. TRS/G-3/2022/2.

### 3.4 Training and Awareness

3.4.1 The MCRBP should provide quarterly reminders, awareness and/or training to all its personnel in identifying and handling phishing and cybersecurity threats.

3.4.2 IT officer(s) of an MCRBP should be given adequate training in ensuring the cybersecurity of its workplace.

3.4.3 The MCRBP is recommended to educate their customers on online financial fraud and the need to protect their personal details and other confidential data.

## 4. IT ASSETS

### 4.1 IT Asset Management

4.1.1 The MCRBP should establish a list of authorised hardware and software options and determine the vendors that are authorised to supply these options.

4.1.2 All IT assets in the MCRBP should be recorded in an IT asset register. The IT asset register should be reviewed on an annual basis and update when there are changes.

4.1.3 The MCRBP should identify which IT assets are critical based on the impact severity if the IT assets become inaccessible, stolen or otherwise.

4.1.4 The personnel of MCRBP should ensure all IT assets are physically secured. Additionally, the personnel of a MCRBP should prevent access or use of work computers by an unauthorised person.

4.1.5 The MCRBP should establish procedures for its personnel to report damaged, lost or stolen IT assets to the IT officer, management, police or other relevant authorities, where applicable.

4.1.6 The MCRBP should have a procedure in place to ensure information or data inside IT assets are fully removed before disposal or change of ownership.

4.1.7 The MCRBP should ensure that all its hardware and software are maintained by the MCRBP's IT officer and/or the vendors/service providers/contractors (if any) to ensure satisfactory performance and security.

4.1.8 All hardware and software licenses should be monitored and renewed by the MCRBP before the expiration date to ensure continued support. The MCRBP should upgrade or replace hardware and software that has reached end of support or end of life.

## 4.2 Data Asset Management

4.2.1 Data should be classified according to sensitivity and confidentiality and the impact severity where such data are exposed or lost. For example, the MCRBP may classify its data as Secret, Confidential and Restricted.

4.2.2 The classification of data should be made aware to the MCRBP's personnel and authorised stakeholders.

4.2.3 The MCRBP should identify data that needs to be classified in accordance with paragraph 4.2.1 above and determine the location(s) where such information should be stored.

4.2.4 The MCRBP should establish a list of approved media and channels for the storage and transmission of classified data. An MCRBP should ensure that classified data is not sent over an email without encryption or password protection.

4.2.5 Critical data on all computers should be backed up using an external hard disk or other approved storage media. The backup media and the data inside the backup media should be encrypted and safely stored in a locked cabinet.

## 4.3 Computer Security

4.3.1 The MCRBP should provide dedicated computers for official work purposes only.

4.3.2 The MCRBP should ensure that its computers are properly secure by ensuring the following:

a) Operating system of all computers are regularly updated;
b) Anti-virus or anti-malware software is installed, activated, running and regularly updated;
c) Only legitimate software is installed on the computers; and
d) Disable or remove unwanted software and features.

4.3.3 The MCRBP should create standard user accounts for each of its personnel who require access to its computers. Only the IT officer should be given administrator access into the MCRBP's computers.

4.3.4 The MCRBP should ensure that its personnel disable access to its computers when leaving it unattended such as by logging off or locking the operating system screen.

4.3.5 The MCRBP should ensure that laptops are not left unattended in open public areas and should only connect to a known and trusted wireless network.

4.3.6 Personal laptop or desktop used for work purpose should be declared as MCRBP's IT asset, and subject to Paragraph 4.3.2 to 4.3.5 above.

## 4.4 Network Security

4.4.1 The MCRBP should ensure their wireless network is secured with at least a WPA2 network key. The network key should be more than 10 digits long and a combination of upper and lower case alphanumeric and special characters.

4.4.2 The MCRBP should ensure that the wireless router's default administrator password has been changed and not to be shared to anyone including vendors.

4.4.3 The MCRBP should implement firewalls to restrict unauthorised network traffic. At a minimum, the MCRBP should ensure that the operating system's firewall on each of its computers are enabled.

4.4.4 Network for back office and server should be separated from high risk devices such as front office computers and personal devices.

## 4.5 Mobile Devices

4.5.1 When mobile devices are required to perform its business operations, the MCRBP should provide dedicated mobile devices to its personnel.

4.5.2 The MCRBP should ensure that its mobile devices are properly secure by ensuring the following:

a) Access to these mobile devices are protected using a passcode or password;
b) The firmware or operating system of the mobile devices are regularly updated;
c) The mobile devices should only contain applications from legitimate and trusted sources; and
d) The mobile devices should be installed with an anti-virus program.

4.5.3 The MCRBP should create user accounts (i.e. Apple or Google account) on the mobile devices. The user accounts should be linked to the MCRBP's email address.

4.5.4 The MCRBP should establish procedures for its personnel to report damaged, lost or stolen mobile devices to the IT officer, management, police or other authority where applicable.

4.5.5 The MCRBP should ensure all sensitive and confidential business data are removed from the mobile devices before transfer of ownership, disposal or otherwise.

## 4.6 Server Management

4.6.1 Servers, including computer that are configured to act as a server should be included in the IT asset register, and listed as critical system.

4.6.2 Servers should be located in a safe and secure room or segregated by partition, separate from the front office.

4.6.3 Firewalls should be used and correctly configured to protect the server from harmful network traffic, and separated from other networks.

4.6.4 The server room should be safe from fire, water, dust, and electrical hazards.

4.6.5 Access to the server room should be strictly restricted to IT officers. Other personnel or vendors needing access should be accompanied by the IT officer.

4.6.6 Air-conditioning and fire alarm should be installed to prevent servers from overheating which may cause fire.

4.6.7 Uninterruptable Power Supply, or UPS is recommended to be installed on most critical server such as database server. In the event of unplanned power outage, the UPS will allow the IT officer to safely shut down the database server, and prevent data loss.

4.6.8 Remote access, whether using Remote Desktop Protocol or third-party application, should be disabled on servers. Temporary remote access can be provided if supervised and recorded by IT officer.

## 5. IT SYSTEMS

### 5.1 Access Control Management

5.1.1 User account creation and deletion in the systems of the MCRBP including change of roles and access permissions should be recorded by the MCRBP. These activities should be subject to the prior approval from the IT officer.

5.1.2 Any system of the MCRBP should have specific and identifiable user accounts for each user. User accounts are personal to the specific user and should not be shared with other users. However, if the system has only one user account for the MCRBP, the user account should be identifiable based on the MCRBP's name, and any personnel who have access to this account should be recorded.

5.1.3 The IT officer should set minimum password requirements for all user accounts, including, but not limited to, requiring a password length of more than 8 characters using a combination of different characters.

5.1.4 Administrator accounts should not be used without proper justification. Administrator accounts should have stronger security measures from a standard user account such as by having complex passwords with more than 12 characters and implementing two-factor authentication.

5.1.5 User access shall be reviewed every six months to verify whether user accounts are still valid. Inactive user accounts or accounts that belong to personnel that is no longer working with the MCRBP should be disabled.

## 5.2 Web Browser Security

5.2.1 The MCRBP should ensure that only fully supported web browsers are allowed to be used in its business operations and the web browsers should be regularly updated to the latest version.

5.2.2 The MCRBP should uninstall or disable any unnecessary and/or unauthorized browser extensions, plug-ins or add-ons.

5.2.3 The MCRBP should disable or block third-party cookies, automatic password storing, tracking, pop-ups and automatic downloads on the web browser.

5.2.4 The MCRBP should ensure that all online user accounts are logged out when not in use.

## 5.3 Email Security

5.3.1 The MCRBP should ensure that only email exchange servers or services approved by the MCRBP are used by its personnel to send out emails.

5.3.2 The MCRBP should ensure that all of its emails are delivered by HTTPS or with SSL.

5.3.3 The MCRBP should create a dedicated email account with an identifiable email address for each personnel. The MCRBP's personnel should not share their email account with any other person.

5.3.4 If the MCRBP is using a single email account for official work purposes, the MCRBP should ensure that the email address is identifiable based on its business name. Any access to the email by its personnel should be recorded.

5.3.5 The MCRBP should ensure that anti-virus software installed on the computer is able to scan email attachments.

## 5.4 Configuration Management

5.4.1 The MCRBP should establish a configuration baseline or standard settings for their computers, networks, servers and systems through reliable benchmarking and configuration guides.

5.4.2 Changes to configuration should be recorded and approved by the IT officer.

## 5.5 Patch Management

5.5.1 The MCRBP should ensure that security patches for systems, servers or applications are applied in a timely manner to address vulnerabilities. These should be provided by the vendor, manufacturer or developer.

5.5.2 If certain vulnerabilities of the MCRBP's systems, servers or applications cannot be resolved due to performance impact or unavailability of security patches from the relevant vendor, manufacturer or developer, the MCRBP should ensure alternative security measures are in place to mitigate any risks.

5.5.3 Patch activities should be recorded and approved by the IT officer. Proper planning should be made to minimise downtime or impact to business operations.

### 5.6 System Security

5.6.1 Specialised systems for MCRBP whether outsource developed, off-the-shelf solutions, provided by counterparty, or Software-as-a-Service (SaaS) should have valid and active contract or service level agreement with the vendor or counterparty.

5.6.2 The system should have sufficient system security by mitigating security vulnerabilities in the system. Vulnerability scan and penetration testing should at least be performed once, and when there are major upgrades to the system.

5.6.3 MCRBP should ensure support service is provided, including provision of regular updates and security patches.

5.6.4 Where system integration between MCRBP's system and counterparty's system is required, an agreement between both parties should be in place, to ensure amongst others the security of both systems.

5.6.5 When changing to new systems, MCRBP should inform and seek BDCB's view on the changes, including the management of risks associated with the changes.

5.6.6 New systems are subjected to a series of testing, including a carefully planned user acceptance test to ensure the system function according to the MCRBP's expectation.

## 6. IT INCIDENTS

### 6.1 Incident Response

6.1.1 The MCRBP should develop communication procedures for its personnel to alert or notify the IT officer, management and stakeholders on any IT incident.

6.1.2 All IT and cybersecurity issues should be recorded and categorized according to their impact. Issues that disrupt or could potentially disrupt the MCRBP's business operations or affect its data should be regarded as an IT incident.

6.1.3 The MCRBP should identify all stakeholders that handle IT incidents, including personnel, vendors, counterparts and local CERT where applicable. Their roles and responsibilities should be made clear and recorded for an effective escalation process.

6.1.4 Major IT incidents that have severe and widespread impact on the MCRBP's operations or has a material impact to the MCRBP should be informed immediately to the management of the MCRBP.

6.1.5 The MCRBP is required to notify BDCB and provide incident reports based on the category of incidents which may occur to the compliance officer. Please refer to the Notice on Early Detection of Cyber Intrusion and Incident Reporting (FTU/N-1/2017/1) on this requirement.

6.1.6 IT incidents that have been resolved should be reviewed by the MCRBP for lessons learnt and the MCRBP should consider resolution of recurring, similar or related incidents.

### 6.2 Business Continuity Management

6.2.1 The MCRBP should establish a proper plan to ensure that it can still continue its business operations during an IT incident.

6.2.2 A proper communication plan, alternative process and workaround method should be prepared by the MCRBP to prevent more loss during an IT incident.

6.2.3 It is recommended for the MCRBP to prepare a reserve computer on standby which can be used during an IT incident to access data and systems. The reserved computer should be prepared with necessary updates, configuration and software.

6.2.4 The MCRBP should ensure that its reserve computer is stored in a safe location and is only accessible by its personnel during an IT incident.

### 6.3 Monitoring and Detection

6.3.1 The MCRBP should have robust capabilities to proactively detect suspicious activities in their network, systems, servers and computers. This can be achieved through implementing suitable monitoring technology such as antivirus programs and firewalls and/or ensuring there are proper internal processes in detecting suspicious activities (for example, transaction monitoring and periodic log review).

6.3.2 The MCRBP should ensure that procedures are put in place to verify and analyse the suspicious activities referred to in paragraph 6.3.1 above. These procedures should also include a process to escalate the matter into an IT incident.

6.3.3 It is important that the MCRBP maintains a keen sense of situational awareness by continuously assessing their technical and internal control processes to improve the capabilities in monitoring and detecting at network, system, server, and computer level.

## 7. DIGITAL CHANNEL

### 7.1 Online Services

7.1.1 MCRBP should implement security and control measures that are commensurate with the risk involved to ensure data confidentiality, integrity, availability and resilience of the online services.

7.1.2 In order to have a secure authentication system in place, MCRBP should consider the following measures:

i. Allow users to choose a longer login password (e.g. up to 12 characters) including alphabet, numerical and special characters unless supported with two-factor authentication;

ii. Provide options to show users how long the password has been in use and to recommend a password update when it reaches a certain period;

iii. Allow a limited number of log-in attempts and if the user fails to enter the correct login details, the online account should be disabled for a certain period to prevent brute force dictionary attack;

iv. MCRBP should also have multi-factor authentication for logging into the online systems;

v. Double confirmation whenever a customer wants to authorise an online transaction (e.g. transferring money, bill payment and cash top up);

vi. Automatic logout after a period of inactivity or when web browser is closed; and

vii. Transmission of sensitive data on the internet should be done via secure and encrypted communications.

7.1.3 MCRBP should secure communication channels by using strong cryptographic controls to safeguard the confidentiality and integrity of confidential data during transmission such as using Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption.

7.1.4 MCRBP should take adequate measures to minimise exposure to its internet services from any cyberattack such as code injection attack, distributed denial of service (DDoS) and spoofing attacks.

7.1.5 MCRBP should provide an option for customers to subscribe to transactions alert (SMS, email, mobile banking) for any account information changes or transactions conducted over the online service.

7.1.6 MCRBP should also perform regular and rigorous testing on the web application or online portal including end to end process and transactions. It is also expected for MCRBP to maintain a log for any change or update to system interface, process and security features of the web application or online portal for audit purposes.

## 7.2 Mobile Application

7.2.1 MCRBP that offer online services via smartphones or tablet devices should be aware of the risks unique to mobile applications. As such, MCRBP should implement specific measures aimed at addressing risks of offering mobile applications.

7.2.2 MCRBP that offer mobile applications should consider additional measures to enhance security of the application, for example as follows:

i. Disable storing or caching data in the mobile application or to clear the data when session ended. If storing of data is necessary for the application, the data should be stored in the local storage of the device instead of sending over to the server, and to be protected using end-to-end encryption;

ii. Implement appropriate application integrity checks to verify the authenticity and integrity of the application;

iii. Implement two-factor authentication, including one-time password (OTP) to set up first log-in and before performing high risk activity (e.g. transaction).

iv. Implement a secure in-app keypad to mitigate against malware that captures keystroke; and

v. Implement mobile device binding to allow only one device to receive software token at one time.

7.2.3 MCRBP should continuously monitor the status of its applications, regularly conduct vulnerability scanning and penetration testing, and perform security update/patching when available.

7.2.4 Distribution of mobile applications or software to customers should only be performed through official mobile application stores or other secure delivery channels.

## 7.3 Social Media

7.3.1 MCRBP may use social media to promote financial products or services, and to make latest announcements relating to their business. Considering social media is powered by a third party, MCRBP should evaluate and determine which social media is suitable.

7.3.2 Social media should only contain information that can be released to the public.

7.3.3 The social media account should be a business account and recommended to be verified if available on the chosen social media platform.

7.3.4 The content of the social media should only be managed by the content administrator. MCRBP should assign one personnel as content administrator.

7.3.5 The social media account should only be used for the business or corporate purposes. The account should not be used for personal purposes and linked to other unrelated services or websites.

7.3.6 Unnecessary features in the social media platform should be disabled, such as personalised advertisement and auto collection of diagnostic data, where the options are available.

7.3.7 MCRBP should monitor and control the profiles followed, friends added, pages liked or groups joined. Where possible, the MCRBP should review their account's followers or friends, and remove or block fake followers or friends.

7.3.8 Comment features should be disabled unless administered by the content administrator. Comments that are potentially harmful or illegal should be removed.

7.3.9 MCRBP should provide official contact details on the social media. If the MCRBP allows instant messaging (IM), direct messaging (DM) or other built-in messengers, the MCRBP should ensure there is dedicated personnel to answer the online queries. Where possible, the MCRBP should direct the public to the official contact channel for further information.

### 7.4 Other Digital Channel

7.4.1 With the advancement in technology, MCRBP should exercise caution and remain proactive in identifying emerging technology and new cyber threats that may be disruptive to their business. It is always expected for MCRBP to conduct risk assessment and analysis whether its current infrastructure and employee's capability are able to manage, control and contain technological threats when introducing new technology or feature into its current business.

7.4.2 For any products or services that uses other form of technology that are not described above, MCRBP should prepare the following:

i. Rationale on the proposal;

ii. Risk assessment and analysis on the new technology and business process;

iii. Strategic roadmap including timeline to address concerns identified after risk assessment and analysis; and

iv. End-to-end process flow, architecture diagram and/or data-flow diagram.

7.4.3 MCRBP should ensure that the product or services are within the allowed services or activities for the MCRBP's license type and legislations relevant to their licenses. The MCRBP should also be able to demonstrate that the offering of new product or services will not diminish the MCRBP's capability to comply with the relevant legislations.

## 8. CONSUMER PROTECTION

### 8.1 Consumer Personal Data Protection

8.1.1 When it is necessary to collect customer's personal data, MCRBP should clearly indicate the purpose of the data collection and have in place a suitable method to obtain consent from the customer.

8.1.2 Data protection or privacy policy should be established or be included in the service terms and conditions. The policy should be made available for the customer to view.

8.1.3 In the event that there are changes to the intended purpose of the data collection, the MCRBP should request for renewed consent from the customer.

8.1.4 MCRBP should not gain consent through force or unsolicited ways. Instead, the MCRBP should communicate the reasons for the data collection, and/or inform the consequences or limitations on the MCRBP's side if the MCRBP is unable to obtain necessary consent to the customer's personal information.

8.1.5 MCRBP should also provide clear disclaimers if their customer-facing system or mobile app automatically collects data such as via cookies, cache or data analytic tool.

8.1.6 MCRBP should ensure the personal data of customers are accurate, current and complete. The MCRBP should establish relevant process to request or allow customers to review and update their personal data.

8.1.7 MCRBP should be able to demonstrate that the storage of customer personal data is secure and when required, to clearly indicate the controls in place to the customers.

8.1.8 When sending over customer personal information such as bank statement or payment receipt online, MCRBP should arrange adequate protection such as encryption to protect the data from unauthorised receivers.

8.1.9 MCRBP should be able to clearly explain on how the MCRBP handle customers' data, including when data is processed in MCRBP's system, or transmitted to a third party. Consent should also be required before sharing or transmission of data, which can be requested during data collection.

8.1.10 If sharing or transmission of data is required to a third party, including storage of personal data on cloud service provider, the purpose should be clearly mentioned to the customers, and the data shared or transmitted should be as minimum as possible for the intended purpose.

8.1.11 Where the third-party is located outside Brunei Darussalam, the MCRBP should ensure personal data protection has been established in that particular country and the third-party has established their own privacy policy.

8.1.12 MCRBP should also be mindful of any applicable statutory or regulatory requirements on data retention, that may include retention of customer personal data. Where necessary, these requirements should be communicated to the customer.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 21 Rabiulawal 1446H / 25 September 2024M