GUIDELINES TO MONEY CHANGER AND MONEY REMITTANCE BUSINESSES

GUIDELINE NO. TRS/G-1/2019/1

STANDARD TECHNOLOGY RISK MANAGEMENT GUIDELINE

---

1. INTRODUCTION

1.1 Innovation and technological developments have transformed the way businesses and operations are being conducted. Financial institutions (FIs) 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. MCRBs are not excluded from such risks. As such, MCRBs need to ensure they have adequate controls to manage these risks.

1.3 This Guideline is issued pursuant to section 32 of the Autoriti Monetari Brunei Darussalam Order, 2010 and aims to provide basic guidance to MCRBs in managing technology and cybersecurity risk based on best industry practices.

1.4 This Guideline is not legally binding, exhaustive and subject to revision from time to time as deemed necessary by the Authority. MCRBs should demonstrate that measures implemented are commensurate with their business model, size, complexity and risk exposure.

1.5 This Guideline shall take effect from 1st January 2020.

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 MCRB'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 MCRB, in which any loss or leak of data will lead to a severe impact to the MCRB'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 MCRB;

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 MCRB's business operations or data;

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

2.1.13 "Material impact" refers to an IT incident which results in severe damage or consequences to an MCRB. 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 MCRB's premise by personnel. This includes, but is not limited to, laptops, tablets and smartphones that are supplied by the MCRB or owned by the personnel;

2.1.15 "Money changer and remittance businesses" or "MCRB" 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 MCRB's work premise that are used in conducting MCRB business activities;

2.1.17 "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;

2.1.18 "Server" refers to server machines that are managed by the MCRB that host their system(s);

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

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

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

2.1.22 "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;

2.1.23 "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

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

3.1.2 The MCRB should mandate all personnel to report 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 MCRB.

3.2 Policy and Procedure

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

3.2.2 The MCRB 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, safeguarding and maintenance of IT assets;
b) Protection, handling and backup of information and data;
c) Handling of IT operations;
d) Issue, complaints and incident handling;
e) User access and password management;
f) Vendor selection, agreement and management.

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

3.2.4 The policies and procedures of the MCRB should be communicated and made available to all personnel in the MCRB.

3.2.5 The management of an MCRB should impose consequences for personnel that violate the policies and procedures of the MCRB.

3.2.6 All system and IT related documentation including administrator guides and user manuals should be kept and stored safely by the MCRB.

3.3 Training and Awareness

3.3.1 The MCRB should provide regular reminders, awareness and/or training to all its personnel on identifying and handling phishing and cybersecurity threats.

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

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

3.4 Third Party Management

3.4.1 The MCRB should ensure that its IT vendors, contractors and service providers are committed in protecting the MCRB's sensitive as well as confidential information and request each of the vendors, contractors and service providers to sign a non-disclosure agreement.

3.4.2 All contracts and agreements with contractors, vendors and service providers relating to information technology should be safely stored and reviewed periodically by the MCRB to maintain validity and ensure consistent performance.

3.4.3 The IT officer of an MCRB should maintain a list of authorised personnel from the vendors, contractors and other service providers and verify their identity before giving access to the MCRB's premises, systems, networks and/or computers. Access to the MCRB's premises, systems, networks and/or computers should only be given to the vendors, contractors and other service provides for the performance of their duties and fulfilment of their obligations as outlined in the relevant contract or agreement.

3.4.4 The MCRB should arrange with the vendors, contractors and service providers a focal contact channel such as by phone, email or helpdesk system to allow the IT officer to report IT issues and request technical assistance.

3.4.5 The MCRB should ensure that the vendors, contractors and service providers provide adequate training and documentation to the IT officer and, where possible, the users on usage of the system (if any).

4. IT ASSETS

4.1 IT Asset Management

4.1.1 The MCRB 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 MCRB should be recorded in an IT asset register. The IT asset register should be reviewed periodically and updated when there are changes.

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

4.1.5 The MCRB 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 MCRB 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 MCRB should ensure that all its hardware and software are maintained by the MCRB'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 MCRB before the expiration date to ensure continued updates and support. The MCRB 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 MCRB may classify its data as Secret, Confidential and Restricted.

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

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

4.2.4 The MCRB should establish a list of approved media and channels for the storage and transmission of classified data. An MCRB 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 MCRB should provide dedicated computers for official work purposes only.

4.3.2 The MCRB 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 are installed on the computers; and
d) Disable or remove unwanted software and features.

4.3.3 The MCRB 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 MCRB's computers.

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

4.4 Network Security

4.4.1 The MCRB should ensure their wireless network is secured with at least a WPA2 network key.

4.4.2 The MCRB should ensure that the wireless router's default administrator password has been changed.

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

4.4.4 The MCRB should not share their wireless network with its customers or the public, unless it is able to provide its customers and/or the public with a separate wireless network.

4.5 Mobile Devices

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

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

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

5. IT SYSTEMS

5.1 Access Control Management

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

5.1.2 Any system of the MCRB should have specific and identifiable user accounts for each users. 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 MCRB, the user account should be identifiable based on the MCRB'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 must be reviewed periodically to verify whether user accounts are still valid. Inactive user accounts or accounts that belong to personnel that is no longer working with the MCRB should be disabled.

5.2 Web Browser Security

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

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

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

5.3 Email Security

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

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

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

5.3.4 If the MCRB is using a single email account for official work purposes, the MCRB 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 MCRB should ensure that anti-virus software installed on the computer is able to scan email attachments.

5.4 Configuration Management

5.4.1 The MCRB 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 MCRB 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 MCRB'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 MCRB should ensure alternative security measures are in place to mitigate any risks.

6. IT INCIDENTS

6.1 Incident Response

6.1.1 The MCRB 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 MCRB's business operations or affect its data should be regarded as an IT incident.

6.1.3 The MCRB 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 MCRB's operations or has a material impact to the MCRB should be informed immediately to the management of the MCRB.

6.1.5 The MCRB is required to notify AMBD 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 MCRB for lessons learnt and the MCRB should consider resolution of recurring, similar or related incidents.

6.2 Business Continuity Management

6.2.1 The MCRB 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 MCRB to prevent more loss during an IT incident.

6.2.3 It is recommended for the MCRB 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 MCRB 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 MCRB 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 MCRB 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 MCRB 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.

MANAGING DIRECTOR
AUTORITI MONETARI BRUNEI DARUSSALAM

Issued Date: 29 Rabiulawal 1441H / 26 November 2019M