

MAS Notice No.: FSM-N06

Notice to banks in Singapore

Financial Services and Markets Act 2022

Issue Date: 09 May 2024

NOTICE ON CYBER HYGIENE

I. Introduction

1.1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the “Act”) and applies to all banks in Singapore (each a “relevant entity”).

II. Definitions

2.1 For the purpose of this Notice----

“administrative account”, means any user account, that has full privileges and unrestricted access to any one or more of the following systems:

- (a) an operating system;
- (b) a database;
- (c) an application;
- (d) a security appliance; or
- (e) a network device;

“banking business” has the meaning given by section 2(1) of the Banking Act 1970;

“bank in Singapore” has the meaning given by section 2(1) of the Banking Act 1970;

“critical system” in relation to a relevant entity, means a system, the failure of which will cause significant disruption to the operations of the relevant entity or materially impact the relevant entity’s service to its customers such as a system which—

- (a) processes transactions that are time critical; or
- (b) provides essential services to customers;

“customer”, in relation to a relevant entity, includes the Monetary Authority of Singapore or any monetary authority or central bank of any other country or territory, and any company which carries on a banking business, a merchant banking business or an investment banking business;

“customer information”, in relation to a relevant entity, means —

- (a) any information relating to, or any particulars of, an account of a customer of the relevant entity, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or
- (b) deposit information;

“deposit information”, in relation to a relevant entity, means any information relating to —

- (a) any deposit of a customer of the relevant entity;
- (b) funds of a customer under management by the relevant entity; or
- (c) any safe deposit box maintained by, or any safe custody arrangements made by, a customer with the relevant entity,

but does not include any information that is not referable to any named person or group of named persons;

“funds of a customer under management” means any funds or assets of a customer (whether of the relevant entity or any financial institution) placed with that relevant entity for the purpose of management or investment;

“multi-factor authentication” means the use of two or more factors to verify an account holder’s claimed identity. Such factors include, but are not limited to—

- (a) something that the account holder knows such as a password or a personal identification number;
- (b) something that the account holder has such as a cryptographic identification device or token;
- (c) something that the account holder is such as an account holder’s biometrics or his behaviour;

“permitted business” has the meaning given by section 55Q of the Banking Act 1970;

“security patch”, in relation to a system, means an update that can be applied to the system to address a vulnerability;

“security standards”, in relation to a system, means a set of configurations for the purpose of safeguarding and improving the security of the system;

“system”, in relation to a relevant entity, means any hardware or software that is used by the relevant entity;

“vulnerability”, in relation to a system, means any weakness, susceptibility or flaw of the system that can be exploited, including but not limited to by allowing an unauthorised person to access the system, or to compromise the security configuration settings of the system.

Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

III. **Application of Notice**

3.1 A relevant entity need not comply with a requirement in this Notice to the extent that it is unable to exercise control over a system to ensure compliance with that requirement, in all of the following ways:

- (a) the relevant entity cannot exercise direct control over the system to ensure compliance with that requirement;
- (b) a relevant entity cannot exercise indirect control over the system by requiring the system provider to ensure compliance with that requirement;
- (c) it is not reasonable for the relevant entity to procure an alternative system provider over whom the relevant entity is able to exercise such indirect control referred to in sub-paragraph (b), to provide the system.

IV. **Cyber Hygiene Practices**

4.1 **Administrative Accounts:** A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account.

4.2 **Security Patches:**

- (a) A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability.

- (b) Where no security patch is available to address a vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system.

4.3 **Security Standards:**

- (a) A relevant entity must ensure that there is a written set of security standards for every system.
- (b) Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards.
- (c) Where the system is unable to conform to the set of security standards, the relevant entity must ensure that controls are instituted to reduce any risk posed by such non-conformity.

4.4 **Network Perimeter Defence:** A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic.

4.5 **Malware protection:** A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented.

4.6 **Multi-factor Authentication:** A relevant entity must ensure that multi-factor authentication is implemented for the following:

- (a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and
- (b) all accounts on any system used by the relevant entity to access customer information through the internet.

V. **Effective Date**

5.1 This Notice shall take effect on 10 May 2024.