

MAS Notice No.: FSM-N22

Notice to capital markets financial institutions

Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on 20 August 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 the following financial institutions:

- (a) approved exchanges under the Securities and Futures Act 2001 (“SFA”)(“AE”);
- (b) recognised market operators under the SFA (“RMO”) which are incorporated in Singapore;
- (c) licensed trade repositories under the SFA (“LTR”);
- (d) approved clearing houses under the SFA (“ACH”);
- (e) recognised clearing houses under the SFA (“RCH”) which are incorporated in Singapore;
- (f) the Depository as defined in section 81SF of the SFA;
- (g) approved holding companies under the SFA (“AHC”);
- (h) holders of a capital markets services licence under the SFA;
- (i) authorised benchmark administrators under the SFA;
- (j) authorised benchmark submitters under the SFA;
- (k) designated benchmark submitters under the SFA;
- (l) trustees for a collective investment scheme authorised under section 286 of the SFA, that are approved under the SFA (each a “relevant entity”).

[FSM-N22 (Amendment) 2024]

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;

“business relations”, in relation to a benchmark administrator, means—

- (a) the collection of information from a person (whether a natural person, legal person or legal arrangement) by the benchmark administrator for the purpose of administering a designated benchmark under the SFA; or
- (b) the provision of a designated benchmark by the benchmark administrator to, a person (whether a natural person, legal person or legal arrangement);

“customer”—

- (a) in relation to an AE, a RMO incorporated in Singapore, a LTR, an ACH and a RCH incorporated in Singapore, includes a user as defined in section 2(1) of the SFA;
- (b) in relation to the Depository, includes a depositor as defined in section 81SF of the SFA;
- (c) in relation to an AHC, includes a user, as defined in section 2(1) of the SFA, of an AE, ACH or LTR, where such AE, ACH or LTR is a subsidiary of the AHC;
- (d) in relation to a holder of a capital markets services licence, includes any “customer” as defined in paragraph (a)(i) of the definition of “customer” in section 2(1) of the SFA and any person with whom the relevant entity, as principal, enters or will enter into transactions for the sale or purchase of capital market products;
- (e) in relation to an authorised benchmark administrator, includes—
 - (i) a person (whether a natural person, legal person or legal arrangement)—
 - (A) who provides information to the benchmark administrator in relation to a designated benchmark; or
 - (B) with whom the benchmark administrator establishes or intends to establish business relations; and
 - (ii) the clients of any person referred to in sub-paragraph (i).
- (f) in relation to an authorised benchmark submitter or designated benchmark submitter, includes a person whose information is collected by the benchmark submitter for the purpose of providing information in relation to a designated benchmark;

- (g) in relation to a trustee for a collective investment scheme authorised under section 286 of the SFA, that is approved under the SFA, includes a manager of the collective investment scheme as defined in section 2(1) of the SFA, and a person who participates in the collective investment scheme by way of owning one or more units in the collective investment scheme;

“customer information” means any information relating to, or any particulars of, any customer of the relevant entity, where a named customer or group of named customers can be identified, or is capable of being identified, from such information;

“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;

“legal arrangement” means a trust or other similar arrangement;

“legal person” means an entity other than a natural person that can establish a permanent customer relationship with a financial institution (as defined in section 123ZZ(2) of the SFA) or otherwise own property;

“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;

“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.

2.2 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.

*Notes on History of Amendments

1. MAS Notice FSM-N22 (Amendment) 2024 with effect from 20 August 2024