MAS Notice No.: FSM-N03

Notice to licensed insurers other than captive insurers and marine mutual insurers
Financial Services and Markets Act 2022

Issue Date: 09 May 2024

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all licensed insurers under the Insurance Act 1966, other than captive insurers and marine mutual insurers (each an "insurer").

Definitions

2 For the purpose of this Notice—

"captive insurer" has the meaning given by section 2 of the Insurance Act 1966;

"critical system" in relation to an insurer, means a system, the failure of which will cause significant disruption to the operations of the insurer or materially impact the insurer's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on, a critical system, or a system which compromises the security, integrity or confidentiality of customer information;

"licensed insurer" has the meaning given by section 2 of the Insurance Act 1966;

"marine mutual insurer" has the meaning given by section 2 of the Insurance Act 1966;

“relevant incident” means a system malfunction or IT security incident, which has a severe and widespread impact on the insurer’s operations or materially impacts the insurer’s service to its customers;

“system” means any hardware, software, network, or other information technology (“IT”) component which is part of an IT infrastructure;

“system malfunction” means a failure of any of the insurer’s critical systems.

3 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.

Technology Risk Management

4 An insurer must put in place a framework and process to identify critical systems.

5 An insurer must make all reasonable effort to maintain high availability for critical systems. The insurer must ensure that the maximum unscheduled downtime for each critical system that affects the insurer’s operations or service to its customers does not exceed a total of 4 hours within any period of 12 months.

6 An insurer must establish a recovery time objective (“RTO”) of not more than 4 hours for each critical system. The RTO is the duration of time, from the point of disruption, within which a system must be restored. The insurer must validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing.

7 An insurer must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

8 An insurer must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain—

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the insurer’s—

i. compliance with laws and regulations applicable to the insurer;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

9 An insurer must implement IT controls to protect customer information from unauthorised access or disclosure.

Effective Date

10 This Notice shall take effect on 10 May 2024.