

Notice No.: PSOA-N05

Issue Date: 21 June 2013

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 20(1) of the Payment Systems (Oversight) Act (Cap. 222A) (the “Act”) and applies to all operators and settlement institutions of designated payment systems (each a “relevant entity”).

Definitions

2 For the purpose of this Notice—

“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;

“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;

“relevant incident” means a system malfunction or IT security incident, which has a severe and widespread impact on the relevant entity’s operations or materially impacts the relevant entity’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 relevant entity’s critical systems.

3 Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires, have the same meaning as in the Act.

Technology Risk Management

4 A relevant entity shall put in place a framework and process to identify critical systems.

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

6 A relevant entity shall 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 relevant entity shall 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 A relevant entity shall notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

8 A relevant entity shall 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 shall 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 relevant entity’s—
 - i. compliance with laws and regulations applicable to the relevant entity;
 - 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 A relevant entity shall implement IT controls to protect customer information from unauthorised access or disclosure.

Effective Date

10 This Notice shall take effect on 1 July 2014.