MAS Notice No.: CBN02

Issue Date: 28 May 2021

NOTICE TO LICENSED CREDIT BUREAUS
CREDIT BUREAU ACT 2016 (ACT 27 OF 2016)

NOTICE ON TECHNOLOGY RISK MANAGEMENT

INTRODUCTION

1. This Notice is issued pursuant to section 75(1) of the Credit Bureau Act 2016 (the "Act") and applies to all licensed credit bureaus.

DEFINITIONS

2. For the purpose of this Notice —

"customer" has the same meaning as in section 2 of the Act but includes any company that carries on banking business, or such other financial institution as may be prescribed under the Act;

"critical system" in relation to a licensed credit bureau, means a system, the failure of which will cause significant disruption to the operations of the licensed credit bureau or materially impact the licensed credit bureau's service to a relevant person, such as a system which –

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

"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 relevant person information;

"relevant incident" means a system malfunction or IT security incident, which has a severe and widespread impact on the licensed credit bureau's operations or materially impacts the licensed credit bureau's service to relevant persons;

"relevant person" means a customer, data subject, or member;

"relevant person information" means any information relating to, or any particulars of, any relevant person, where a named relevant person or group of named relevant persons can be identified, or is capable of being identified, from such information;

"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 licensed credit bureau'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 licensed credit bureau must put in place a framework and process to identify critical systems.

5. A licensed credit bureau must make all reasonable efforts to maintain high availability for critical systems. The licensed credit bureau must ensure that the maximum unscheduled downtime for each critical system that affects the licensed credit bureau's operations or service to its relevant persons does not exceed a total of 4 hours within any period of 12 months.

6. A licensed credit bureau 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 licensed credit bureau 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. A licensed credit bureau must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

8. A licensed credit bureau 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 licensed credit bureau's —

(i) compliance with laws and regulations applicable to the licensed credit bureau;
(ii) operations; and
(iii) service to relevant persons; and

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

9. A licensed credit bureau must implement IT controls to protect relevant person information from unauthorised access or disclosure.

Effective Date

10. This Notice shall take effect on 31 May 2021.